PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-157237
(43)Date of publication of application : 30.05.2003

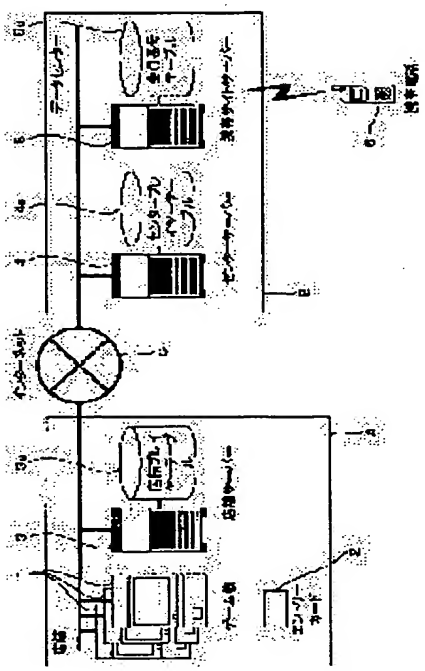
(51)Int.Cl. G06F 15/00
H04Q 7/38
// A63F 13/12

(21)Application number : 2001-355349
(22)Date of filing : 20.11.2001

(71)Applicant : KONAMI CO LTD
(72)Inventor : TAKAHASHI KAZUYA
SUGANO HIROSHI
NAKAMURA MASARU

(54) NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the security of issuing and inputting information needed to make user data available from a personal terminal such as a portable telephone and also to provide a user with the information at a low cost.
SOLUTION: User identification information for utilizing a general terminal 1 is made to correspond to the user data of the user to be stored in a storing means 4. If the personal terminal 6 makes access accompanied with a request for password issuing, access identification information unique to the user notified accompanying the access is acquired, a password determined unequivocally to the access identification information is issued, and the password is reported to the personal terminal 6. If the password and the user identification information are associated with each other and inputted in the general terminal 1, association with the access identification information corresponding to the inputted password is set with the user data stored in the storing means 4 as a target corresponding to the inputted user identification information.



LEGAL STATUS

[Date of request for examination] 20.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The user data generated for every user based on the contents for which each of two or more users used the common terminal installed considering use by the unspecified user as a premise A storage means to match with the user-identification information for specifying each user, and to memorize, When there is access accompanied by the issue demand of a password from the individual terminal which each user uses individually, The password management tool which publishes the password which acquired the access identification information of the user proper notified with the access, and was uniquely defined to the access identification information, A notice means of a password to notify the published password to said individual terminal, When said password and said user-identification information related and are mutually inputted at said general terminal, It is aimed at said user data with which said storage means memorizes the entered password and user-identification information from a common terminal corresponding to reception and its received user-identification information. The network system characterized by having a correlation setting means to set up correlation with the access identification information corresponding to the received password.
[Claim 2] Said correlation setting means is a network system according to claim 1 characterized by setting up correlation with said user data and said access identification information by matching and recording said user-identification information or the user data corresponding to the user-identification information, and said password.
[Claim 3] The network system according to claim 2 characterized by having further a user data specification means for said password management tool to specify the password corresponding to the access identification information notified with the access, and to specify the user data corresponding to the specified password when there is access accompanied by the predetermined demand about said user data from said individual terminal.
[Claim 4] Said password management tool is a network system according to claim 3 characterized by constituting said predetermined processing so that predetermined processing may be performed to said access identification information, said password may be generated and the same password may be generated to the same access identification information.
[Claim 5] A user data extraction means to extract said user data by which an injury setup with relation is carried out among the user data recorded on said storage means, The password recorded by matching with the extracted user data and correspondence relation with said access identification information are used. An access identification information specification means to specify the access identification information corresponding to said extracted user data, A network system given in any 1 term of claims 2-4 characterized by having the distribution control means which distributes predetermined information to the individual terminal corresponding to the specified access identification information.
[Claim 6] A network system given in any 1 term of claims 1-5 characterized by having a prohibition means to forbid resetting of said correlation by said correlation setting means about the user data with which said correlation is already set up.
[Claim 7] An R/W means for it to be prepared in said general terminal and to perform writing of said user-identification information to a predetermined record medium, and reading of the written-in user-identification information, and when said user-identification information is not recorded on said record medium An issue means to publish user-identification information, and an initial-data record means to match the published user-identification information with predetermined initial user data, and to record on said record means, A preparation, a network WASHI stem given in any 1 term of claims 1-6 characterized by writing the published user-identification information in said record medium through said R/W means.
[Claim 8] The user data generated for every user based on the contents for which each of two or more users used the common terminal installed considering use by the unspecified user as a premise The user data control equipment which holds the database which matched with the user-identification information for specifying each user, and was recorded, answers the Request to Send accompanied by said user recognition information, and transmits the user data corresponding to the recognition information, The network service offer equipment with which it connects through the individual terminal and network which are used individually, and a member offers predetermined service to access accompanied by the access identification information from said individual terminal, It provides. Said network service offer equipment The password management tool which publishes the most important password from said individual terminal to the access identification information notified with the access when there is access accompanied by the issue demand of a password, A notice means of a password to notify the published password to said individual terminal, A password offer means to provide said user data control equipment

with the password corresponding to the access identification information of the member who answers a user data use demand from said individual terminal, and uses the individual terminal, When it provided, and said user-identification information and said password associated said user data control equipment mutually and it is inputted at said general terminal, A correlation setting means to set up correlation with the user data corresponding to reception and its received user-identification information for the user-identification information and password which were entered, and said password on said database from a common terminal side, When said password is offered from said network service offer equipment, The network system characterized by having the data use control means which specifies the user data related with the offered password, and enables use on said individual terminal about the specified user data.

[Claim 9] Answer access from said individual terminal and the terminal identification information on a proper is specified as the individual terminal. Said individual terminal includes the specific individual terminal connected to said network service offer equipment through the predetermined communication processing system which attaches the specified terminal identification information and notifies the contents of access. Said network service offer equipment holds the member information table which matched said terminal identification information and the member identification information for every member accepted in the service provision range from said network service offer equipment. When there is access from said specific individual terminal Acquire said terminal identification information as said access identification information, and said member information table is referred to. It is the network system according to claim 8 which possesses a member information management means to specify the member identification information corresponding to the acquired access identification information, and is characterized by said password management tool publishing said password based on said member identification information.

[Claim 10] The writing of said user-identification information to a record medium predetermined to said general terminal, An R/W means to perform reading of the written-in user-identification information, and an issue demand means to output an issue demand of user-identification information when user-identification information effective in said record medium is not recorded are established. The user-identification information management equipment with which publishes new user-identification information according to the demand from said issue demand means, and said general terminal and said user data control equipment are provided is formed in said network system. Said user data control equipment acquires said new user-identification information from said user-identification information management equipment. The acquired user-identification information is matched with predetermined initial user data, and it records on said database. Said R/W means of said general terminal The network system according to claim 8 or 9 characterized by what the user-identification information is recorded for on said record medium when said new user-identification information is acquired from said user-identification information management equipment.

[Claim 11] It is the network system according to claim 10 which said user data control equipment is installed in common with the common terminal of two or more of said stores, and said user-identification information management equipment is between the common terminal of each store, and said user data control equipment, and is characterized by being prepared for every store while said general terminal is installed in each of two or more stores.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the network system which can connect a common terminal and an individual terminal through a network.
[0002]
[Description of the Prior Art] While a user creates game data based on the contents played at the game terminal of a game center and saves the game data to a predetermined server, the game system which a user accesses the server from individual terminals, such as a cellular phone, and makes game data available is known.
[0003] In such a game system, it is necessary to specify with which game data the user who accessed from the individual terminal corresponds. While the server which generated the password at the game terminal, transmitted to the server with game data as an approach of specifying such correspondence relation, and received this matches and saves a password and game data Display the password on the screen of a game machine, in case a user accesses a server from an individual terminal, the password is made to enter, and how to specify game data using the entered password can be considered.
[0004] The card with which unique ID was beforehand recorded as the other approaches, and that ID was printed is prepared beforehand, and there is the approach of selling this card to the user of a game terminal. A user purchases a card, inserts the card in a game machine, and plays a game. A game machine transmits ID recorded on the card to read in, and transmits the ID to a server with game data. A server matches and saves ID and game data which were transmitted. A user can access the game data of self by accessing a server from individual terminals, such as a cellular phone, and inputting ID printed by the card.
[0005]
[Problem(s) to be Solved by the Invention] However, in displaying a password on the screen of the common terminal installed in the location in which many and unspecified users have gathered like a game center, there is a possibility that a password may be stolen by others. Moreover, it is necessary to record unique ID on the card before crossing to a user's hand beforehand, and to print the same ID as it on a card by the approach of using an above-mentioned card. Therefore, manufacture and management of a card take time and effort, and it becomes the factor which pushes up the selling price of a card.
[0006] Then, the safety for [the user data recorded by being generated based on the contents of use of a common terminal, and matching with user-identification information] issue and the input of information required since [terminals /, such as a different cellular phone from a common terminal, / individual] it is available is high, and this invention aims at offering the network system which can provide a user with such information by low cost.
[0007]
[Means for Solving the Problem] Hereafter, this invention is explained. In addition, although the reference mark of an accompanying drawing is written in addition in parenthesis writing in order to make an understanding of this invention easy, thereby, this invention is not limited to the gestalt of illustration.
[0008] The network system of this invention the user data generated for every user based on the contents for which each of two or more users used the common terminal (1) installed considering use by the unspecified user as a premise A storage means to match with the user-identification information for specifying each user, and to memorize (4), When there is access accompanied by the issue demand of a password from the individual terminal (6) which each user uses individually, The password management tool which publishes the password which acquired the access identification information of the user proper notified with the access, and was uniquely defined to the access identification information (5), A notice means of a password to notify the published password to said individual terminal (5), When said password and said user-identification information related and are mutually inputted at said general terminal, It is aimed at said user data with which said storage means memorizes the entered password and user-identification information from a common terminal corresponding to reception and its received user-identification information. The technical problem mentioned above is solved by having a correlation setting means (4) to set up correlation with the access identification information corresponding to the received password.
[0009] According to the network system of this invention, a password functions as information required in order to make available the user data currently recorded on user-identification information by matching from an individual terminal. That is, access identification information and user data are associated through a password. Since a network system publishes a password suitably, it does not require time and effort which distributes to a user the card with which unique ID was beforehand recorded and the ID was printed, but can provide a user with a password

by low cost. A password is displayed on the individual terminal concerning a user's individual treatment instead of a common terminal. Therefore, as compared with the case where a password is displayed on the screen of the common terminal which many and unspecified users use, possibility that a password will be stolen by other users is low for whether your being Haruka, and is so high. [of the safety about issue of a password] If a password is related with user-identification information and entered into a common terminal, since the user data corresponding to the inputted user-identification information will be targetted for an injury setup with relation of the access identification information corresponding to a password, a password is only used inside a system after it as a medium which matches access identification information and user data. The correspondence relation between user data and access identification information is distinguished through a password, and if information other than the password for specifying the distinguished correspondence relation is recorded on the storage means, it will become unnecessary or to be able to deduce user data now from access identification information through information other than the password, and to use a password, in case correlation is set up. For this reason, it is necessary to enter a password neither from a common terminal nor an individual terminal again. Therefore, safety is high also about the input of a password.

[0010] In addition, a common terminal contains various kinds of computer machines. Furthermore, this invention is suitable, when it is installed in a commercial facility and many and unspecified users use an available device as a common terminal like the arcade game machine installed in a game center, the personal computer installed in an Internet cafe, and the training machine installed in sport crab. However, the profit for the purpose of [of a common terminal] installation and non-profit do not ask. An individual terminal contains various kinds of computer machines which have a network connection function. Furthermore, a cellular phone, PDA, and the information machines and equipment constituted considering individual use like a handheld game machine as a premise are used as an individual terminal. The personal computer and video game equipment which are installed in domestic can also be used as an individual terminal. However, it does not ask whether an individual terminal is applied to possession of a user. As a matter of fact, if a user is the computer machine used individually, it is usable as an individual terminal.

[0011] A password management tool may publish the most important password to access identification information by generating the most important password, extracting any one password from the password group defined beforehand, and matching with access identification information with a predetermined algorithm. The notice means of a password may notify a password using a character string, and may notify a password with a sound signal.

[0012] Said correlation setting means can set up correlation with said user data and access identification information by matching and recording the password thought to be said user-identification information or user data corresponding to the user-identification information. in this case, the injury with relation — it can set up easily.

[0013] However, a correlation setting means may match other information defined still more nearly uniquely corresponding to the received password with user data, and may record it. The information uniquely defined to a password may be generated by processing a password with a predetermined algorithm. It matches with user-identification information or user data, and the candidate of the information which should be recorded can be prepared partly beforehand and the information uniquely defined from the password can be generated also by approach which receives the received password, shifts and assigns that candidate uniquely.

[0014] When a correlation setting means matches a password with user data and records it, the still more nearly following modes are possible.

[0015] When there is access accompanied by the predetermined demand about said user data from said individual terminal, you may make it have further a user data specification means (4) for said password management tool to specify the password corresponding to the access identification information notified with the access, and to specify the user data corresponding to the specified password. In this case, when there is access as which a password management tool specifies user data through a password from a means to publish a password in response to the password issue demand from an individual terminal, and an individual terminal [finishing / password issue], it is made to serve a double purpose as a means to specify a password from access identification information. Thereby, password management is unified and the time and effort of information management is mitigated.

[0016] Said predetermined processing may be constituted so that said password management tool may perform predetermined processing to said access identification information, and may generate said password and the same password may be generated to the same access identification information. In this case, even if it does not independently record the correspondence relation between a password and access identification information, the same password is acquirable from access identification information. Therefore, the storage capacity of a storage means can be saved. In addition, predetermined processing may include the check code for incorrect input prevention in a password so that it may encipher access identification information.

[0017] A user data extraction means to extract said user data by which an injury setup with relation is carried out among the user data recorded on said storage means (4), The correspondence relation between said password recorded on the extracted user data by matching and said access identification information is used. A network system may be further equipped with an access identification information specification means (5) to specify the access identification information corresponding to said extracted user data, and the distribution control means (5) which distributes predetermined information to the individual terminal corresponding to the specified access identification information. In this case, only to the user who entered the password notified to the individual terminal from the common terminal, predetermined information is distributed and that information is not distributed to the user who is not inputted [password unissued or]. Therefore, the motivation which accesses from an individual terminal, and acquires a password, and enters the password can be given to a user, and use of the system of this

invention can be urged.
[0018] In the network system of this invention, you may have a prohibition means (5) to forbid resetting of said correlation by said correlation setting means about the user data with which said correlation is already set up. In this case, if a password is entered and an injury setup with relation is carried out from a common terminal, even if it associates the same user-identification information and the same password and inputs into a common terminal after that, an injury change with relation will not be made. Therefore, even if the password under input is read by others, there is no damage, and the safety about the input of a password increases further.
[0019] An R/W means for it to be prepared in said general terminal (1), and to perform writing of said user-identification information to a predetermined record medium (2), and reading of the written-in user-identification information in the network system of this invention, An issue means to publish user-identification information when said user-identification information is not recorded on said record medium (3), It is good also as a thing equipped with an initial-data record means (4) to match the published user-identification information with predetermined initial user data, and to record on said record means by which the published user-identification information is written in said record medium through said R/W means. In this case, before a record medium passes into a user, it is not necessary to record unique ID on a record medium. Therefore, a record medium can be manufactured cheaply. Moreover, since information is written in after a user purchases, a user can be made to employ a record medium flexibly.
[0020] Other network systems of this invention the user data generated for every user based on the contents for which each of two or more users used the common terminal (1) installed considering use by the unspecified user as a premise The database (4a) which matched with the user-identification information for specifying each user, and was recorded is held. The user data control equipment which answers the Request to Send accompanied by said user recognition information, and transmits the user data corresponding to the recognition information (4), The network service offer equipment with which it connects through the individual terminal (6) and network which are used individually, and a member offers predetermined service to access accompanied by the access identification information from said individual terminal (5), It provides. Said network service offer equipment (5) The password management tool which publishes the most important password to the access identification information notified with the access when there is access accompanied by the issue demand of a password from said individual terminal, A notice means of a password to notify the published password to said individual terminal, A password offer means to provide said user data control equipment with the password corresponding to the access identification information of the member who answers a data use demand from said individual terminal, and uses the individual terminal, It provides. Said user data control equipment (4) When said user-identification information and said password related and are mutually entered at said general terminal, A correlation setting means to set up correlation with the user data corresponding to reception and its received user-identification information for the user-identification information and password which were entered, and said password on said database from a common terminal side, When said password is offered from said network service offer equipment, The technical problem mentioned above is solved by having specified the user data related with the offered password, and having had the data use control means which enables use on said individual terminal about the specified user data.
[0021] In this network system, user data control equipment can support use of a user's common terminal, and network service offer equipment can offer not only use of a common terminal but various services to a member. Since user data control equipment holds the database which matched user-identification information and user data, a user can read and use the user data of self for a common terminal from user data control equipment by making user-identification information into a key. Network service offer equipment publishes the password corresponding to access identification information, and notifies it to an individual terminal, and when the password relates with user-identification information and is entered at a common terminal, user data control equipment receives such passwords and user-identification information, and sets up correlation with user data and a password on a database. Thereby, if it is the member for receiving the service from network service offer equipment, the user data based on the contents using a common terminal can be used from the individual terminal of self. Network service offer equipment publishes a password suitably, and the password is notified to the individual terminal concerning a user's individual use. Since user data and access identification information are matched, a password is used with network service offer equipment and user data control equipment, or it becomes unnecessary furthermore, to use it, if it inputs once at a common terminal. Therefore, like the network system described previously, a user can be provided with a password by low cost, and the safety about issue and the input of a password is high.
[0022] In addition, also in this network system, a common terminal contains various kinds of computer machines with which a game is performed. Furthermore, this invention is suitable, when it is installed in a commercial facility. and many and unspecified users use an available device as a common terminal like the arcade game machine installed in a game center, the personal computer installed in an Internet cafe, and the training machine installed in sport crab. However, the profit for the purpose of [of a common terminal] installation and non-profit do not ask. An individual terminal contains various kinds of computer machines which have a network connection function. Furthermore, a cellular phone, PDA, and the information machines and equipment constituted considering individual use like a handheld game machine as a premise are used as an individual terminal. The personal computer and video game equipment which are installed in domestic can also be used as an individual terminal. However, it does not ask whether an individual terminal is applied to possession of a user. As a matter of fact, if a user is the computer machine used individually, it is usable as an individual terminal.
[0023] A password management tool may publish the most important password to access identification information

by generating the most important password, extracting any one password from the password group defined beforehand, and matching with access identification information with a predetermined algorithm. The notice means of a password may notify a password using a character string, and may notify a password with a sound signal.
[0024] Use of the user data on an individual terminal contains various kinds of modes, such as actuation of perusal of user data, edit of user data, etc., and a play of the game on the individual terminal based on the user data about a game.
[0025] in other network systems of this invention, said individual terminal should answer access from an individual terminal, should specify the terminal identification information on a proper as the individual terminal, and should meet the specified terminal identification information — the specific individual terminal connected to said network service offer equipment through the predetermined communication processing system which notifies the contents of ** access can be included. For example, the cellular phone which has an Internet connectivity function is connected to the site on a network through such a communication processing system. When it includes such a specific individual terminal, said network service offer equipment (5) The member information table (5a) which matched said terminal identification information and the member identification information for every member accepted in the service provision range from said network service offer equipment is held. When there is access from said specific individual terminal Acquire said terminal identification information as said access identification information, and said member information table is referred to. A member information management means to specify the member identification information corresponding to the acquired access identification information is provided, and, as for said password management tool, it is desirable to publish said password based on said member identification information. Since the terminal identification information notified with access from a specific individual terminal is used in order to differ from the purpose which enables use of the user data from an individual terminal essentially, various technical or commercial constraint generates such information to match with user data, or it has a possibility that a certain legal restrictions may arise. On the other hand, terminal identification information can be changed into member identification information, and use of publishing a password based on the member identification information, then the terminal identification information in a network system can be stopped to the minimum. And since member identification information itself is not matched user data and directly but member identification information and user data are indirectly associated so to speak through a password, even if a password is stolen by others at the time of the input of a common terminal etc., even member identification information is not known. Thereby, a possibility that it may be spoiled by the addition of the function of use of user data does not have the safety of various kinds of services using network service offer equipment, either.
[0026] The writing of said user-identification information to a record medium (2) predetermined to said general terminal, An R/W means to perform reading of the written-in user-identification information, and an issue demand means to output an issue demand of user-identification information when user-identification information effective in said record medium is not recorded are established. The user-identification information management equipment (3) with which publishes new user-identification information according to the demand from said issue demand means, and said general terminal and said user data control equipment are provided is formed in said network system. Said user data control equipment (4) acquires said new user-identification information from said user-identification information management equipment. The acquired user-identification information is matched with predetermined initial user data, and it records on said database (4a). Said R/W means of said general terminal when said new user-identification information is acquired from said user-identification information management equipment, the user-identification information is recorded on said record medium — it is good even if like. In this case, since it is not necessary to record unique ID on a record medium before a record medium passes into a user, a record medium can be manufactured cheaply. Moreover, since information is written in a record medium after a user purchases, a user can be made to employ a record medium flexibly. Furthermore, while said general terminal is installed in each of two or more stores, said user data control equipment is installed in common with the common terminal of two or more of said stores, and said user-identification information management equipment is between the common terminal of each store, and said user data control equipment, and may be formed for every store.
[0027]
[Embodiment of the Invention] Drawing 1 is drawing showing the network game structure of a system concerning 1 operation gestalt of this invention. This game system connects a data center B with Internet C to many stores A, and is constituted. The data center B is carrying out package management of the game data generated at each store A. For this reason, a user can use the game data of self played at Store A also at other stores A. Moreover, the data center B is managing the website of an accessible membership system from the cellular phone 6. The data center B provides the member with various services, such as download service of game software, and offer of event information. As one of the service of the, the predetermined service about the game played at Store A is also offered. For example, the user who is the member of a website can use the game data of self played at Store A by accessing a data center B through a network from individual terminals, such as a cellular phone 6.
[0028] Two or more game machines (equivalent to a common terminal) 1—1 are installed in each store A. A user inserts the entry card 2 containing record media, such as a magnetic tape and IC, in one of the game machines 1, and starts a game. A game machine 1 reads ID as user-identification information currently recorded on the entry card 2, and provides a user with the game based on the player data (equivalent to the game data for every user) corresponding to the ID. Player data are different data for every user generated including the information about ID, and the information based on a user's game hysteresis. The detail of player data is mentioned later. Each game machine 1 is connected with the store server (user-identification information management equipment) 3 installed in

each store one set through networks, such as LAN. The store server 3 is recording the player data used at the self store on store player table 3a. The store server 3 is connected to the pin center,large server (game data control equipment) 4 installed in the data center through networks, such as the Internet. The pin center,large server 4 is recording the player data used at all stores on pin center,large player table 4a. The pin center,large server 4 is connected to the pocket site server 5 installed in the data center through networks, such as LAN. The pocket site server (network service offer equipment) 5 is managing the website of an accessible membership system from the cellular phone 6. The pocket site server 5 is recording the information about a member on member number table 5a.

[0029] Drawing 2 (a) shows the contents of member number table 5a. The cellular phone ID for specifying the owner of the cellular phone 6 accessed to the pocket site server (access identification information, instrument identification information) and the member number (member identification information) of the website which a pocket site server manages match, and are recorded on member number table 5a. When a user accesses the pocket site server 5 from a cellular phone 6, the pocket site server 5 is notified of cellular phone ID by the telephone company, and it is the value of a proper for every cellular phone. If the telephone company has the dispatch from a cellular phone 6, it will specify the carrying ID of the cellular phone 6, and will manage the communications processing network (un-illustrating) of which attaches the cellular phone ID to the information corresponding to the contents of access from a cellular phone 6, and the pocket site server 5 is notified.

[0030] Drawing 2 (b) shows the contents of store player table 3a and pin center,large player table 4a. The player data recorded on each table include the information about ID, the information about the date (time) by which player data were updated, the information about the password uniquely generated from a member number, and the information about the condition of a character. The information which shows the condition of a character includes the information about the identifier of a character, level, the item to own. In addition, when a password is invalid (not registered yet), the information about a password serves as NULL.

[0031] Drawing 3 is a flow chart which shows the procedure of the password issue processing which a cellular phone 6 and the pocket site server 5 perform, respectively. This processing is started, when a cellular phone 6 accesses the pocket site server 5 and issue of a password is required. If a user performs predetermined actuation to a cellular phone 6, a cellular phone 6 will transmit a password issue demand to the pocket site server 5 (step S601), and will wait for transmission of a password at step S602 after that. The pocket site server 5 which received the password issue demand specifies a member number from the carrying ID of a cellular phone 6 which transmitted the password issue demand (step S501). In addition, when a cellular phone 6 accesses the pocket site server 5, the pocket site server 5 is notified of the cellular phone ID from the telephone company. Next, by enciphering the member number, the password which becomes settled uniquely to a member number is generated (step S502), and it transmits to a cellular phone 6 (step S503). A cellular phone 6 will display the password on a screen, for example like Screen 10 of drawing 4 , if a password is received (step S603). Thereby, a user acquires the password corresponding to a self cellular phone.

[0032] Drawing 5 is a flow chart which shows the procedure of processing from the game initiation which a game machine 1 performs to termination. This processing is started by performing predetermined actuation for game initiation while the entry card 2 is inserted in a game machine 1 by the user. First, a game machine 1 judges whether ID is recorded on the entry card 2 (step S101). When it judges with ID not being recorded, ID issue demand is transmitted to the store server 3 (step S102). That is, it is judged as the first play and first time registration processing is required of the store server 3. About processing of the store server 3 which received ID issue demand, it mentions later. A game machine 1 waits to transmit the player data of the initial state which contains unique ID from the store server 3 at step S103. When player data are received, ID contained in the player data is written in the entry card 2 (step S104). Next, processing for making a user customize the player data is performed (step S105), and the customized player data are transmitted to the store server 3 (step S106).

[0033] When it judges with ID being recorded on the entry card 2 at step S101, the ID is transmitted to the store server 3 (step S107). That is, it is judged as the play of the 2nd henceforth and transmission of the player data corresponding to the ID is required. About processing of the store server 3 which received ID, it mentions later. A game machine 1 waits to transmit the player data corresponding to ID which transmitted from the store server 3 at step S108. When it receives, it progresses to step S109.

[0034] At step S109, processing for making a user play a game is performed based on player data. When it comes to game over, the player data changed according to the advance situation of a game are transmitted to the store server 3 (step S110), and processing is ended.

[0035] Drawing 6 is a flow chart which shows the procedure of the first time registration processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID issue demand (step S102 reference of drawing 5) transmitted from the game machine 1. The store server 3 creates the player data of the initial state containing the ID while publishing unique ID, if ID issue demand is received from a game machine 1 (step S301). Next, the player data is transmitted to a game machine 1 (step S302). The transmitted data are received by the game machine 1 which was standing by at step S103 of drawing 5 . If a game machine 1 transmits player data at step S106 (drawing 5), the store server 3 which was standing by to reception of the player data at step S303 of drawing 6 will attach the date (time) to the player data, and will record on store player table 3a (step S304). In addition, the part which should record the information about a password is considered as the invalid mark, and serves as NULL (refer to drawing 2 (b)). Next, the player data is transmitted to the pin center,large server 4 (step S305). The pin center,large server 4 records the received player data on pin center,large player table 4a (step S401), and transmits the information about the recorded time to the store server 3 (step S402). Based on the

received time, the store server 3 which was standing by to reception of the information about time at step S306 corrects the time of the player data recorded at step S304 (step S307), and ends first time registration processing.
[0036] Drawing 7 is a flow chart which shows the procedure of the data transmitting processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID (step S107 reference of drawing 5) transmitted from the game machine 1. The store server 3 which received ID from the game machine 1 judges whether the player data corresponding to the ID are recorded on store player table 3a (step S311). When it judges with transmitting the player data to the pin center,large server 4 (step S312), and not being recorded, when it judges with being recorded, the ID is transmitted to the pin center,large server 4 (step S313). The pin center,large server 4 judges whether ID was received for whether player data were received (step S411). When it judges with having received player data, the player data corresponding to ID contained in the received player data are searched from pin center,large player table 4a, the date of player data which received is compared with the date of the player data currently recorded on pin center,large player table 4a, and any judge whether it is new data (step S412). When it judges with the received player data being newer, the player data of pin center,large player table 4a are updated (step S413), and the sign of "O.K." is transmitted to the store server 3 (step S414). When it judges with having received ID at step S411, the player data corresponding to the ID are searched from pin center,large player table 4a, and it transmits to the store server 3 (step S415). Moreover, also when it judges with it being newer than the player data which the direction of the player data currently recorded on pin center,large player table 4a at step S412 received, the player data currently recorded on pin center,large player table 4a are transmitted (step S415). The store server 3 which was waiting for the result of the data enquiry from the pin center,large server 4 at step S314 judges whether the sign of "O.K." was received for whether player data were received at step S315. When it judges with having received player data, store player table 3a is updated with the received player data (step S316). Then, the player data is transmitted to a game machine 1 (step S317). At step S315, when it judges with having received the sign of "O.K.", step S316 is skipped and player data are transmitted to a game machine 1 (step S317). The player data transmitted at step S317 are received by the game machine 1 which was standing by at step S108 of drawing 5 .
[0037] Drawing 8 is a flow chart which shows the procedure of the password registration processing which a game machine 1 performs. When predetermined actuation for matching the member number of the website which the pocket site server 6 manages, and ID recorded on the entry card 2 is performed, this processing is started while the entry card 2 is inserted in a game machine 1 by the user. First, a game machine 1 reads the information about ID recorded on the entry card 2, and it judges whether ID is recorded or not (step S121). Processing is ended if ID is not recorded. When ID is recorded, processing for making a user enter a password is performed, and it judges whether the password was entered or not (step S122). Processing is ended when a password input is canceled. When a password is entered, it judges whether the entered password is effective (step S123). That is, a user judges whether the random password is entered. Therefore, in step S502 of drawing 3 , the password is generated, such as including the alphabetic character for error checking in a password, so that it can detect from a password whether the password is effective. Processing is ended when it judges with a password not being effective at step S123 of drawing 8 . When it judges with it being effective, ID and a password are transmitted to the store server 3 (step S124). When ID and a password are received, about the processing which the store server 3 performs, it mentions later. When waiting (step S125) and a registration result are received for the result of whether to have registered the password from the store server 3, a game machine 1 ends processing, after it displays the result on a user.
[0038] Drawing 9 is a flow chart which shows the procedure of the password registration processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID, the password, and (step S124 reference of drawing 8) which were transmitted from the game machine 1. The store server 3 transmits ID and the password which were received to the pin center,large server 4 (step S321). The pin center,large server 4 searches the player data corresponding to ID which received from pin center,large server 4a (step S421). Next, it judges whether the information about the password of the corresponding player data is NULL (step S422). In being NULL, the received password is recorded as information about the password of the player data (step S423), and it transmits the sign of a password registration success to the store server 3 (step S424). At step S422, when it judges with the information about a password not being NULL, step S423 is skipped and the sign of a registered purport is already transmitted to the store server 3 (step S424). At step S322, when it judges with a registration result being the sign of a success, the store server 3 which was waiting for the registration result searches the player data with which store player table 3a corresponds, and records the password (step S324). Next, the sign of a password registration success is transmitted to a game machine 1 at a game machine 1 (step S325). When a registration result judges with the sign of an already registered purport at step S323, step S324 is skipped and the sign of a registered purport is already transmitted to a game machine 1 (step S325). The transmitted registration result is received by the game machine 1 which was standing by at step S125 of drawing 8 .
[0039] Drawing 10 is a flow chart which shows the procedure of the data transmitting processing which the pin center,large server 4 and the pocket site server 5 perform. This processing is started when a user makes demands for transmission of the player data of self by predetermined actuation on the pocket site server 5 from a cellular phone 6. When there is a Request to Send of player data from a user, the pocket site server 5 specifies the member number corresponding to cellular phone ID (step S531). Next, by the same encryption approach as step 502 of drawing 3 , the password which becomes settled uniquely for the member number is created (step S532), and it transmits to the pin center,large server 4 (step S533). The pin center,large server 4 which received the password searches the player data containing the password from pin center,large player table 4a (step S431). Next, the

corresponding player data are transmitted to the pocket site server 5 (step S432). The pocket site server 5 which was waiting for transmission of player data at step S534 transmits the received player data to the cellular phone 6 of the user who demanded transmission (step S535).

[0040] or [in addition, / that the information concerning / the pin center,large server 4 / a password is effective] -- the existence of a pocket site admission privilege may be judged by whether it is an invalid (NULL). For example, admission to a pocket site can be demanded from the user of the registered cellular phone 6 according to the privilege of publishing e-mail. Moreover, in steps S423 and S324, using the information which becomes settled uniquely instead of a password based on passwords, such as information which enciphered the password further, after it, as no password is used, security may be raised further.

[0041] Drawing 11 - drawing 18 illustrate processing to drawing 3 - drawing 9 . The case where a new user starts a game hereafter from the condition shown in drawing 11 is mentioned as an example, and processing of the network game system of this invention is explained further.

[0042] As for drawing 11 , ID shows the situation that the player data of 1-3 are recorded to store player table 3a and store player table 4a.

[0043] Drawing 12 shows the user 50 with the new pocket site server 5 the situation when publishing a password (refer to drawing 3 and drawing 4). A user 50 is the member of the website which the pocket site server 5 is managing, and makes demands for password issue on the pocket site server 5 from a cellular phone 6. The pocket site server 5 which received the demand publishes a password, and makes it display on a cellular phone 6.

[0044] Drawing 13 and drawing 14 show the game machine 1 in case a user 50 plays for the first time with a game machine 1, and each server's situation (refer to drawing 5 and drawing 6). In drawing 13 , a user throws in coin and inserts the intact (ID is not recorded yet) entry card 2 in a game machine 1. A game machine 1 detects that ID is not recorded on the entry card 2 yet, and transmits ID issue demand to the store server 3. The store server 3 creates the player data containing the ID, and transmits to a game machine 1 while he publishes ID. In drawing 14 , the player data which the user customized are transmitted to the store server 3 from a game machine 1. The store server 3 attaches the date to the data, and records on store player server 3a. In this drawing, the player data of ID=4 are newly added as a user's 50 player data. In addition, the column of a password serves as NULL as an invalid mark at this time. The store server 3 transmits this player data to the pin center,large server 4. The pin center,large server 4 records the received player data on pin center,large player table 4a. Next, the pin center,large server 4 transmits the date to the store server 3. The store server 3 corrects the date of the player data of ID=4 currently recorded on store player table 3a.

[0045] Drawing 15 and drawing 16 show the game machine 1 and the situation of each server, when a user 50 registers a password (refer to drawing 8 and drawing 9). In drawing 15 , a user 50 enters a password while inserting the entry card 2 in a game machine 1. ID read in the password and the entry card 2 is transmitted to the pin center,large server 4 via the store server 3 from a game machine 1. The pin center,large server 4 searches the player data with which this ID is contained. If the column of the password of the corresponding player data is NULL, a password will be recorded there (this drawing ID= 4 player data). In drawing 16 , as for the pin center,large server 4, registration of a password notifies the store server 3 of a success or failure. If it is a success, the store server 3 will record a password on the player data of ID=4 of store player table 3a. As for the store player server 3, registration of a password notifies a success or failure to a game machine 1 at a game machine 1.

[0046] Drawing 17 and drawing 18 show the game machine 1 and each server's situation, when a user 50 plays 2nd henceforth (refer to drawing 5 and drawing 7). In drawing 17 , a user 50 puts coin into a game machine 1, and inserts an entry card. If password registration has already finished, it is not necessary to enter a password. A game machine 1 reads ID in the entry card 2 (this drawing ID= 4), and requires the player data containing the ID of the store server 3. If the store server 3 has player data applicable to store player table 3a and there is about the player data, he will transmit ID to the pin center,large server 4, and will demand player data. [no] The pin center,large server 4 reads the corresponding player data (ID=4) from pin center,large player table 4a. In drawing 18 , the pin center,large server 4 transmits player data etc. according to the demand advanced by drawing 17 by the store server 3. That is, when player data are received from the store server 3, the date of player data which received is compared with the date of the player data with which pin center,large server 4a corresponds, and the sign of "O.K." will be transmitted if the player data which received the player data when the pin center,large server 4a was newer are newer. When ID is received from the store server 3, the player data with which pin center,large server 4a corresponds are transmitted. In addition, the sign of "BAD" is transmitted when a certain error of there being no player data applicable to pin center,large server 4a occurs. The store server 3 transmits the player data of store player table 3a to a game machine 1, when "O.K." is received. When player data are received, while recording the player data on store player table 3a (updating), it transmits to a game machine 1.

[0047] As mentioned above, according to this operation gestalt, a member number for processing of step S423 and step S324 (drawing 9) to receive ID for playing a game using player data with a game machine 1 and service of the website which the pocket site server 5 manages is matched with a password. Since a password is published by the pocket site server 5 when a user demands issue from a cellular phone 6 (step S502 of drawing 3), it is not necessary to print and manufacture and sell it on the entry card 2. Moreover, since a password is displayed on the screen of a cellular phone 6 (step S603 of drawing 3), it does not have a possibility that it may be stolen by other users as compared with the case where it displays on a game machine 1. Furthermore, if it inputs into a game machine 1 once at step S122 (drawing 8), since ID and a member number are matched, this password is only used inside a game system, and it is not necessary to enter it from a game machine 1 and a cellular phone 6 any more.

Therefore, the network game system which can realize the high user authentication system of security cheaply can be offered.

[0048] In addition, this invention is not limited to the above operation gestalt, but may be carried out with various gestalten. For example, the store server 3, the pin center,large server 4 and the pin center,large server 4, and the pocket site server 5 may unify, and may unify these three. On the contrary, each server may be distributed further and each server's burden may be mitigated. A game machine 1 may perform issue of ID, and generation of the player data of an initial state. The function as a junction monitor of a game advance situation may be included in the store server 3, and the function which carries out unitary management of the game advance situation, and the function to transmit a game advance situation to each store server 3 may be included in the pin center,large server 4. The function to check whether the received password exists to the pocket site server 5 may be included in the pin center,large server 4. The entry card 2 is not restricted to the thing using the MAG and IC, but just records ID. ID may be recorded on the entry card from the beginning. A password is not restricted to the thing based on a member number, but may be directly generated from cellular phone ID that what is necessary is just what specifies the user who receives service at an individual terminal. Moreover, even if it is not what enciphered the information which specifies a user, if a password does not have the information which specifies a user from a password by other users recognized, it is good. For example, you may enable it to refer to a password from a member number by matching the password with a member number and recording it, using as a password the character string which made it generate at random.

[0049] The network system of this invention is not limited to what uses a game machine or a game terminal as a common terminal, but can be applied to various applications. For example, when the training machine of sport crab is set up as a common terminal, the user data (for example, movement time amount, consumption energy) based on the contents of use of the training machine are recorded on a database, and this invention can be applied also when making the user data available from individual terminals, such as a cellular phone. In this case, a use gestalt which it considers as reference of selection of the contents of a meal, or the contents of a meal actually took in with reference to movement time amount etc. for example, on the individual terminal are transmit [gestalt] from an individual terminal, and a database is update [gestalt], and makes user's individual's everyday life reflect in the decision of the training menu in sport crab by that cause is possible for use of the user data from an individual terminal.

[0050]

[Effect of the Invention] As explained above, according to this invention, access identification information and user data are associated through a password. In order that a system may publish the password suitably, it can provide for a user by low cost. Since a password is displayed on the individual terminal concerning a user's individual treatment, once possibility that a password will be stolen by other users is low and a password is entered into a common terminal A password is used inside a system as a medium which matches access identification information and user data, or it completely ceases to be used, and it is necessary to enter a password again neither from a common terminal nor an individual terminal. Therefore, it is generated based on the contents of use of a common terminal, and the safety for [the user data recorded by matching with user-identification information] issue and the input of information (password) required since [terminals /, such as a different cellular phone from a common terminal, / individual] it is available is high, and the network system which can provide a user with such information by low cost can be realized.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the network system which can connect a common terminal and an individual terminal through a network.

[Translation done.]

PRIOR ART

[Description of the Prior Art] While a user creates game data based on the contents played at the game terminal of a game center and saves the game data to a predetermined server, the game system which a user accesses the server from individual terminals, such as a cellular phone, and makes game data available is known.
[0003] In such a game system, it is necessary to specify with which game data the user who accessed from the individual terminal corresponds. As an approach of specifying such correspondence relation, a game terminal generates a password and it is game data. It transmits to a server, and display the password on the screen of a game machine, in case a user accesses a server from an individual terminal, the password is made to enter, while the server which received this matched and saves a password and game data, and how to specify game data using the entered password can be considered.
[0004] The card with which unique ID was beforehand recorded as the other approaches, and that ID was printed is prepared beforehand, and there is the approach of selling this card to the user of a game terminal. A user purchases a card, inserts the card in a game machine, and plays a game. A game machine transmits ID recorded on the card to read in, and transmits the ID to a server with game data. A server matches and saves ID and game data which were transmitted. A user can access the game data of self by accessing a server from individual terminals, such as a cellular phone, and inputting ID printed by the card.

[Translation done.]

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, in order that according to this invention access identification information and user data may be associated through a password and a system may publish the password suitably A password is used inside a system as a medium which matches access identification information and user data once possibility that a password will be stolen by other users since it is displayed on the individual terminal who can provide for a user by low cost and requires a password for a user's individual treatment was low and the password was entered into the common terminal, or it completely ceases to be used, and it is not necessary to enter a password again from a common terminal and individual terminal. Therefore, it is generated based on the contents of use of a common terminal, and the safety for [the user data recorded by matching with user-identification information] issue and the input of information (password) required since [terminals /, such as a different cellular phone from a common terminal, / individual] it is available is high, and the network system which can provide a user with such information by low cost can be realized.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, in displaying a password on the screen of the common terminal installed in the location in which many and unspecified users have gathered like a game center, there is a possibility that a password may be stolen by others. Moreover, it is necessary to record unique ID on the card before crossing to a user's hand beforehand, and to print the same ID as it on a card by the approach of using an above-mentioned card. Therefore, manufacture and management of a card take time and effort, and it becomes the factor which pushes up the selling price of a card.
[0006] Then, the safety for [the user data recorded by being generated based on the contents of use of a common terminal, and matching with user-identification information] issue and the input of information required since [terminals /, such as a different cellular phone from a common terminal, / individual] it is available is high, and this invention aims at offering the network system which can provide a user with such information by low cost.

[Translation done.]

* NOTICES *

MEANS

[Means for Solving the Problem] Hereafter, this invention is explained. In addition, although the reference mark of an accompanying drawing is written in addition in parenthesis writing in order to make an understanding of this invention easy, thereby, this invention is not limited to the gestalt of illustration.
[0008] The network system of this invention the user data generated for every user based on the contents for which each of two or more users used the common terminal (1) installed considering use by the unspecified user as a premise A storage means to match with the user-identification information for specifying each user, and to memorize (4). When there is access accompanied by the issue demand of a password from the individual terminal (6) which each user uses individually, The password management tool which publishes the password which acquired the access identification information of the user proper notified with the access, and was uniquely defined to the access identification information (5), A notice means of a password to notify the published password to said individual terminal (5), When said password and said user-identification information related and are mutually inputted at said general terminal, It is aimed at said user data with which said storage means memorizes the entered password and user-identification information from a common terminal corresponding to reception and its received user-identification information. The technical problem mentioned above is solved by having a correlation setting means (4) to set up correlation with the access identification information corresponding to the received password.
[0009] According to the network system of this invention, a password functions as information required in order to make available the user data currently recorded on user-identification information by matching from an individual terminal. That is, access identification information and user data are associated through a password. Since a network system publishes a password suitably, it does not require time and effort which distributes to a user the card with which unique ID was beforehand recorded and the ID was printed, but can provide a user with a password by low cost. A password is displayed on the individual terminal concerning a user's individual treatment instead of a common terminal. Therefore, as compared with the case where a password is displayed on the screen of the common terminal which many and unspecified users use, possibility that a password will be stolen by other users is low for whether your being Haruka, and is so high. [of the safety about issue of a password] If a password is related with user-identification information and entered into a common terminal, since the user data corresponding to the inputted user-identification information will be targetted for an injury setup with relation of the access identification information corresponding to a password, a password is only used inside a system after it as a medium which matches access identification information and user data. The correspondence relation between user data and access identification information is distinguished through a password, and if information other than the password for specifying the distinguished correspondence relation is recorded on the storage means, it will become unnecessary or to be able to deduce user data now from access identification information through information other than the password, and to use a password, in case correlation is set up. For this reason, it is necessary to enter a password neither from a common terminal nor an individual terminal again. Therefore, safety is high also about the input of a password.
[0010] In addition, a common terminal contains various kinds of computer machines. Furthermore, this invention is suitable, when it is installed in a commercial facility and many and unspecified users use an available device as a common terminal like the arcade game machine installed in a game center, the personal computer installed in an Internet cafe, and the training machine installed in sport crab. However, the profit for the purpose of [of a common terminal] installation and non-profit do not ask. An individual terminal contains various kinds of computer machines which have a network connection function. Furthermore, a cellular phone, PDA, and the information machines and equipment constituted considering individual use like a handheld game machine as a premise are used as an individual terminal. The personal computer and video game equipment which are installed in domestic can also be used as an individual terminal. However, it does not ask whether an individual terminal is applied to possession of a user. As a matter of fact, if a user is the computer machine used individually, it is usable as an individual terminal.
[0011] A password management tool may publish the most important password to access identification information by generating the most important password, extracting any one password from the password group defined beforehand, and matching with access identification information with a predetermined algorithm. The notice means of a password may notify a password using a character string, and may notify a password with a sound signal.
[0012] Said correlation setting means can set up correlation with said user data and access identification information by matching and recording the password thought to be said user-identification information or user data corresponding to the user-identification information. in this case, the injury with relation — it can set up easily.
[0013] However, a correlation setting means may match other information defined still more nearly uniquely

corresponding to the received password with user data, and may record it. The information uniquely defined to a password may be generated by processing a password with a predetermined algorithm. It matches with user-identification information or user data, and the candidate of the information which should be recorded can be prepared partly beforehand and the information uniquely defined from the password can be generated also by approach which receives the received password, shifts and assigns that candidate uniquely.
[0014] When a correlation setting means matches a password with user data and records it, the still more nearly following modes are possible.
[0015] When there is access accompanied by the predetermined demand about said user data from said individual terminal, you may make it have further a user data specification means (4) for said password management tool to specify the password corresponding to the access identification information notified with the access, and to specify the user data corresponding to the specified password. In this case, when there is access as which a password management tool specifies user data through a password from a means to publish a password in response to the password issue demand from an individual terminal, and an individual terminal [finishing / password issue], it is made to serve a double purpose as a means to specify a password from access identification information. Thereby, password management is unified and the time and effort of information management is mitigated.
[0016] Said predetermined processing may be constituted so that said password management tool may perform predetermined processing to said access identification information, and may generate said password and the same password may be generated to the same access identification information. In this case, even if it does not independently record the correspondence relation between a password and access identification information, the same password is acquirable from access identification information. Therefore, the storage capacity of a storage means can be saved. In addition, predetermined processing may include the check code for incorrect input prevention in a password so that it may encipher access identification information.
[0017] A user data extraction means to extract said user data by which an injury setup with relation is carried out among the user data recorded on said storage means (4), The correspondence relation between said password recorded on the extracted user data by matching and said access identification information is used. A network system may be further equipped with an access identification information specification means (5) to specify the access identification information corresponding to said extracted user data, and the distribution control means (5) which distributes predetermined information to the individual terminal corresponding to the specified access identification information. In this case, only to the user who entered the password notified to the individual terminal from the common terminal, predetermined information is distributed and that information is not distributed to the user who is not inputted [password unissued or]. Therefore, the motivation which accesses from an individual terminal, and acquires a password, and enters the password can be given to a user, and use of the system of this invention can be urged.
[0018] In the network system of this invention, you may have a prohibition means (5) to forbid resetting of said correlation by said correlation setting means about the user data with which said correlation is already set up. In this case, if a password is entered and an injury setup with relation is carried out from a common terminal, even if it associates the same user-identification information and the same password and inputs into a common terminal after that, an injury change with relation will not be made. Therefore, even if the password under input is read by others, there is no damage, and the safety about the input of a password increases further.
[0019] An R/W means for it to be prepared in said general terminal (1), and to perform writing of said user-identification information to a predetermined record medium (2), and reading of the written-in user-identification information in the network system of this invention, An issue means to publish user-identification information when said user-identification information is not recorded on said record medium (3), It is good also as a thing equipped with an initial-data record means (4) to match the published user-identification information with predetermined initial user data, and to record on said record means by which the published user-identification information is written in said record medium through said R/W means. In this case, before a record medium passes into a user, it is not necessary to record unique ID on a record medium. Therefore, a record medium can be manufactured cheaply. Moreover, since information is written in after a user purchases, a user can be made to employ a record medium flexibly.
[0020] Other network systems of this invention the user data generated for every user based on the contents for which each of two or more users used the common terminal (1) installed considering use by the unspecified user as a premise The database (4a) which matched with the user-identification information for specifying each user, and was recorded is held. The user data control equipment which answers the Request to Send accompanied by said user recognition information, and transmits the user data corresponding to the recognition information (4), The network service offer equipment with which it connects through the individual terminal (6) and network which are used individually, and a member offers predetermined service to access accompanied by the access identification information from said individual terminal (5), It provides. Said network service offer equipment (5) The password management tool which publishes the most important password to the access identification information notified with the access when there is access accompanied by the issue demand of a password from said individual terminal, A notice means of a password to notify the published password to said individual terminal, A password offer means to provide said user data control equipment with the password corresponding to the access identification information of the member who answers a data use demand from said individual terminal, and uses the individual terminal, It provides. Said user data control equipment (4) When said user-identification information and said password related and are mutually entered at said general terminal, A correlation setting means to set up correlation with the user

data corresponding to reception and its received user-identification information for the user-identification information and password which were entered, and said password on said database from a common terminal side, When said password is offered from said network service offer equipment, The technical problem mentioned above is solved by having specified the user data related with the offered password, and having had the data use control means which enables use on said individual terminal about the specified user data.

[0021] In this network system, user data control equipment can support use of a user's common terminal, and network service offer equipment can offer not only use of a common terminal but various services to a member. Since user data control equipment holds the database which matched user-identification information and user data, a user can read and use the user data of self for a common terminal from user data control equipment by making user-identification information into a key. Network service offer equipment publishes the password corresponding to access identification information, and notifies it to an individual terminal, and when the password relates with user-identification information and is entered at a common terminal, user data control equipment receives such passwords and user-identification information, and sets up correlation with user data and a password on a database. Thereby, if it is the member for receiving the service from network service offer equipment, the user data based on the contents using a common terminal can be used from the individual terminal of self. Network service offer equipment publishes a password suitably, and the password is notified to the individual terminal concerning a user's individual use. Since user data and access identification information are matched, a password is used with network service offer equipment and user data control equipment, or it becomes unnecessary furthermore, to use it, if it inputs once at a common terminal. Therefore, like the network system described previously, a user can be provided with a password by low cost, and the safety about issue and the input of a password is high.

[0022] In addition, also in this network system, a common terminal contains various kinds of computer machines with which a game is performed. Furthermore, this invention is suitable, when it is installed in a commercial facility and many and unspecified users use an available device as a common terminal like the arcade game machine installed in a game center, the personal computer installed in an Internet cafe, and the training machine installed in sport crab. However, the profit for the purpose of [of a common terminal] installation and non-profit do not ask. An individual terminal contains various kinds of computer machines which have a network connection function. Furthermore, a cellular phone, PDA, and the information machines and equipment constituted considering individual use like a handheld game machine as a premise are used as an individual terminal. The personal computer and video game equipment which are installed in domestic can also be used as an individual terminal. However, it does not ask whether an individual terminal is applied to possession of a user. As a matter of fact, if a user is the computer machine used individually, it is usable as an individual terminal.

[0023] A password management tool may publish the most important password to access identification information by generating the most important password, extracting any one password from the password group defined beforehand, and matching with access identification information with a predetermined algorithm. The notice means of a password may notify a password using a character string, and may notify a password with a sound signal.

[0024] Use of the user data on an individual terminal contains various kinds of modes, such as actuation of perusal of user data, edit of user data, etc., and a play of the game on the individual terminal based on the user data about a game.

[0025] in other network systems of this invention, said individual terminal should answer access from an individual terminal, should specify the terminal identification information on a proper as the individual terminal, and should meet the specified terminal identification information -- the specific individual terminal connected to said network service offer equipment through the predetermined communication processing system which notifies the contents of ** access can be included. For example, the cellular phone which has an Internet connectivity function is connected to the site on a network through such a communication processing system. When it includes such a specific individual terminal, said network service offer equipment (5) The member information table (5a) which matched said terminal identification information and the member identification information for every member accepted in the service provision range from said network service offer equipment is held. When there is access from said specific individual terminal Acquire said terminal identification information as said access identification information, and said member information table is referred to. A member information management means to specify the member identification information corresponding to the acquired access identification information is provided, and, as for said password management tool, it is desirable to publish said password based on said member identification information. Since the terminal identification information notified with access from a specific individual terminal is used in order to differ from the purpose which enables use of the user data from an individual terminal essentially, various technical or commercial constraint generates such information to match with user data, or it has a possibility that a certain legal restrictions may arise. On the other hand, terminal identification information can be changed into member identification information, and use of publishing a password based on the member identification information, then the terminal identification information in a network system can be stopped to the minimum. And since member identification information itself is not matched user data and directly but member identification information and user data are indirectly associated so to speak through a password, even if a password is stolen by others at the time of the input of a common terminal etc., even member identification information is not known. Thereby, a possibility that it may be spoiled by the addition of the function of use of user data does not have the safety of various kinds of services using network service offer equipment, either.

[0026] The writing of said user-identification information to a record medium (2) predetermined to said general terminal, An R/W means to perform reading of the written-in user-identification information, and an issue demand

means to output an issue demand of user-identification information when user-identification information effective in said record medium is not recorded are established. The user-identification information management equipment (3) with which publishes new user-identification information according to the demand from said issue demand means, and said general terminal and said user data control equipment are provided is formed in said network system. Said user data control equipment (4) acquires said new user-identification information from said user-identification information management equipment. The acquired user-identification information is matched with predetermined initial user data, and it records on said database (4a). Said R/W means of said general terminal when said new user-identification information is acquired from said user-identification information management equipment, the user-identification information is recorded on said record medium — it is good even if like. In this case, since it is not necessary to record unique ID on a record medium before a record medium passes into a user, a record medium can be manufactured cheaply. Moreover, since information is written in a record medium after a user purchases, a user can be made to employ a record medium flexibly. Furthermore, while said general terminal is installed in each of two or more stores, said user data control equipment is installed in common with the common terminal of two or more of said stores, and said user-identification information management equipment is between the common terminal of each store, and said user data control equipment, and may be formed for every store.

[0027]

[Embodiment of the Invention] Drawing 1 is drawing showing the network game structure of a system concerning 1 operation gestalt of this invention. This game system connects a data center B with Internet C to many stores A, and is constituted. The data center B is carrying out package management of the game data generated at each store A. For this reason, a user can use the game data of self played at Store A also at other stores A. Moreover, the data center B is managing the website of an accessible membership system from the cellular phone 6. The data center B provides the member with various services, such as download service of game software, and offer of event information. As one of the service of the, the predetermined service about the game played at Store A is also offered. For example, the user who is the member of a website can use the game data of self played at Store A by accessing a data center B through a network from individual terminals, such as a cellular phone 6.

[0028] Two or more game machines (equivalent to a common terminal) 1—1 are installed in each store A. A user inserts the entry card 2 containing record media, such as a magnetic tape and IC, in one of the game machines 1, and starts a game. A game machine 1 reads ID as user-identification information currently recorded on the entry card 2, and provides a user with the game based on the player data (equivalent to the game data for every user) corresponding to the ID. Player data are different data for every user generated including the information about ID, and the information based on a user's game hysteresis. The detail of player data is mentioned later. Each game machine 1 is connected with the store server (user-identification information management equipment) 3 installed in each store one set through networks, such as LAN. The store server 3 is recording the player data used at the self store on store player table 3a. The store server 3 is connected to the pin center,large server (game data control equipment) 4 installed in the data center through networks, such as the Internet. The pin center,large server 4 is recording the player data used at all stores on pin center,large player table 4a. The pin center,large server 4 is connected to the pocket site server 5 installed in the data center through networks, such as LAN. The pocket site server (network service offer equipment) 5 is managing the website of an accessible membership system from the cellular phone 6. The pocket site server 5 is recording the information about a member on member number table 5a.

[0029] Drawing 2 (a) shows the contents of member number table 5a. The cellular phone ID for specifying the owner of the cellular phone 6 accessed to the pocket site server (access identification information, instrument identification information) and the member number (member identification information) of the website which a pocket site server manages match, and are recorded on member number table 5a. When a user accesses the pocket site server 5 from a cellular phone 6, the pocket site server 5 is notified of cellular phone ID by the telephone company, and it is the value of a proper for every cellular phone. If the telephone company has the dispatch from a cellular phone 6, it will specify the carrying ID of the cellular phone 6,, and will manage the communications processing network (un-illustrating) of which attaches the cellular phone ID to the information corresponding to the contents of access from a cellular phone 6, and the pocket site server 5 is notified.

[0030] Drawing 2 (b) shows the contents of store player table 3a and pin center,large player table 4a. The player data recorded on each table include the information about ID, the information about the date (time) by which player data were updated, the information about the password uniquely generated from a member number, and the information about the condition of a character. The information which shows the condition of a character includes the information about the identifier of a character, level, the item to own. In addition, when a password is invalid (not registered yet), the information about a password serves as NULL.

[0031] Drawing 3 is a flow chart which shows the procedure of the password issue processing which a cellular phone 6 and the pocket site server 5 perform, respectively. This processing is started, when a cellular phone 6 accesses the pocket site server 5 and issue of a password is required. If a user performs predetermined actuation to a cellular phone 6, a cellular phone 6 will transmit a password issue demand to the pocket site server 5 (step S601), and will wait for transmission of a password at step S602 after that. The pocket site server 5 which received the password issue demand specifies a member number from the carrying ID of a cellular phone 6 which transmitted the password issue demand (step S501). In addition, when a cellular phone 6 accesses the pocket site server 5, the pocket site server 5 is notified of the cellular phone ID from the telephone company. Next, by enciphering the member number, the password which becomes settled uniquely to a member number is generated (step S502), and it transmits to a cellular phone 6 (step S503). A cellular phone 6 will display the password on a screen, for example like Screen 10 of

drawing 4 , if a password is received (step S603). Thereby, a user acquires the password corresponding to a self cellular phone.

[0032] Drawing 5 is a flow chart which shows the procedure of processing from the game initiation which a game machine 1 performs to termination. This processing is started by performing predetermined actuation for game initiation while the entry card 2 is inserted in a game machine 1 by the user. First, a game machine 1 judges whether ID is recorded on the entry card 2 (step S101). When it judges with ID not being recorded, ID issue demand is transmitted to the store server 3 (step S102). That is, it is judged as the first play and first time registration processing is required of the store server 3. About processing of the store server 3 which received ID issue demand, it mentions later. A game machine 1 waits to transmit the player data of the initial state which contains unique ID from the store server 3 at step S103. When player data are received, ID contained in the player data is written in the entry card 2 (step S104). Next, processing for making a user customize the player data is performed (step S105), and the customized player data are transmitted to the store server 3 (step S106).

[0033] When it judges with ID being recorded on the entry card 2 at step S101, the ID is transmitted to the store server 3 (step S107). That is, it is judged as the play of the 2nd henceforth and transmission of the player data corresponding to the ID is required. About processing of the store server 3 which received ID, it mentions later. A game machine 1 waits to transmit the player data corresponding to ID which transmitted from the store server 3 at step S108. When it receives, it progresses to step S109.

[0034] At step S109, processing for making a user play a game is performed based on player data. When it comes to game over, the player data changed according to the advance situation of a game are transmitted to the store server 3 (step S110), and processing is ended.

[0035] Drawing 6 is a flow chart which shows the procedure of the first time registration processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID issue demand (step S102 reference of drawing 5) transmitted from the game machine 1. The store server 3 creates the player data of the initial state containing the ID while publishing unique ID, if ID issue demand is received from a game machine 1 (step S301). Next, the player data is transmitted to a game machine 1 (step S302). The transmitted data are received by the game machine 1 which was standing by at step S103 of drawing 5 . If a game machine 1 transmits player data at step S106 (drawing 5), the store server 3 which was standing by to reception of the player data at step S303 of drawing 6 will attach the date (time) to the player data, and will record on store player table 3a (step S304). In addition, the part which should record the information about a password is considered as the invalid mark, and serves as NULL (refer to drawing 2 (b)). Next, the player data is transmitted to the pin center,large server 4 (step S305). The pin center,large server 4 records the received player data on pin center,large player table 4a (step S401), and transmits the information about the recorded time to the store server 3 (step S402). Based on the received time, the store server 3 which was standing by to reception of the information about time at step S306 corrects the time of the player data recorded at step S304 (step S307), and ends first time registration processing.

[0036] Drawing 7 is a flow chart which shows the procedure of the data transmitting processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID (step S107 reference of drawing 5) transmitted from the game machine 1. The store server 3 which received ID from the game machine 1 judges whether the player data corresponding to the ID are recorded on store player table 3a (step S311). When it judges with transmitting the player data to the pin center,large server 4 (step S312), and not being recorded, when it judges with being recorded, the ID is transmitted to the pin center,large server 4 (step S313). The pin center,large server 4 judges whether ID was received for whether player data were received (step S411). When it judges with having received player data, the player data corresponding to ID contained in the received player data are searched from pin center,large player table 4a, the date of player data which received is compared with the date of the player data currently recorded on pin center,large player table 4a, and any judge whether it is new data (step S412). When it judges with the received player data being newer, the player data of pin center,large player table 4a are updated (step S413), and the sign of "O.K." is transmitted to the store server 3 (step S414). When it judges with having received ID at step S411, the player data corresponding to the ID are searched from pin center,large player table 4a, and it transmits to the store server 3 (step S415). Moreover, also when it judges with it being newer than the player data which the direction of the player data currently recorded on pin center,large player table 4a at step S412 received, the player data currently recorded on pin center,large player table 4a are transmitted (step S415). The store server 3 which was waiting for the result of the data enquiry from the pin center,large server 4 at step S314 judges whether the sign of "O.K." was received for whether player data were received at step S315. When it judges with having received player data, store player table 3a is updated with the received player data (step S316). Then, the player data is transmitted to a game machine 1 (step S317). At step S315, when it judges with having received the sign of "O.K.", step S316 is skipped and player data are transmitted to a game machine 1 (step S317). The player data transmitted at step S317 are received by the game machine 1 which was standing by at step S108 of drawing 5 .

[0037] Drawing 8 is a flow chart which shows the procedure of the password registration processing which a game machine 1 performs. When predetermined actuation for matching the member number of the website which the pocket site server 6 manages, and ID recorded on the entry card 2 is performed, this processing is started while the entry card 2 is inserted in a game machine 1 by the user. First, a game machine 1 reads the information about ID recorded on the entry card 2, and it judges whether ID is recorded or not (step S121). Processing is ended if ID is not recorded. When ID is recorded, processing for making a user enter a password is performed, and it judges whether the password was entered or not (step S122). Processing is ended when a password input is canceled.

When a password is entered, it judges whether the entered password is effective (step S123). That is, a user judges whether the random password is entered. Therefore, in step S502 of drawing 3 , the password is generated, such as including the alphabetic character for error checking in a password, so that it can detect from a password whether the password is effective. Processing is ended when it judges with a password not being effective at step S123 of drawing 8 . When it judges with it being effective, ID and a password are transmitted to the store server 3 (step S124). When ID and a password are received, about the processing which the store server 3 performs, it mentions later. When waiting (step S125) and a registration result are received for the result of whether to have registered the password from the store server 3, a game machine 1 ends processing, after it displays the result on a user.

[0038] Drawing 9 is a flow chart which shows the procedure of the password registration processing which the store server 3 and the pin center,large server 4 perform. This processing is started when the store server 3 receives ID, the password, and (step S124 reference of drawing 8) which were transmitted from the game machine 1. The store server 3 transmits ID and the password which were received to the pin center,large server 4 (step S321). The pin center,large server 4 searches the player data corresponding to ID which received from pin center,large server 4a (step S421). Next, it judges whether the information about the password of the corresponding player data is NULL (step S422). In being NULL, the received password is recorded as information about the password of the player data (step S423), and it transmits the sign of a password registration success to the store server 3 (step S424). At step S422, when it judges with the information about a password not being NULL, step S423 is skipped and the sign of a registered purport is already transmitted to the store server 3 (step S424). At step S322, when it judges with a registration result being the sign of a success, the store server 3 which was waiting for the registration result searches the player data with which store player table 3a corresponds, and records the password (step S324). Next, the sign of a password registration success is transmitted to a game machine 1 at a game machine 1 (step S325). When a registration result judges with the sign of an already registered purport at step S323, step S324 is skipped and the sign of a registered purport is already transmitted to a game machine 1 (step S325). The transmitted registration result is received by the game machine 1 which was standing by at step S125 of drawing 8 .

[0039] Drawing 10 is a flow chart which shows the procedure of the data transmitting processing which the pin center,large server 4 and the pocket site server 5 perform. This processing is started when a user makes demands for transmission of the player data of self by predetermined actuation on the pocket site server 5 from a cellular phone 6. When there is a Request to Send of player data from a user, the pocket site server 5 specifies the member number corresponding to cellular phone ID (step S531). Next, by the same encryption approach as step 502 of drawing 3 , the password which becomes settled uniquely for the member number is created (step S532), and it transmits to the pin center,large server 4 (step S533). The pin center,large server 4 which received the password searches the player data containing the password from pin center,large player table 4a (step S431). Next, the corresponding player data are transmitted to the pocket site server 5 (step S432). The pocket site server 5 which was waiting for transmission of player data at step S534 transmits the received player data to the cellular phone 6 of the user who demanded transmission (step S535).

[0040] or [in addition, / that the information concerning / the pin center,large server 4 / a password is effective] -- the existence of a pocket site admission privilege may be judged by whether it is an invalid (NULL). For example, admission to a pocket site can be demanded from the user of the registered cellular phone 6 according to the privilege of publishing e-mail. Moreover, in steps S423 and S324, using the information which becomes settled uniquely instead of a password based on passwords, such as information which enciphered the password further, after it, as no password is used, security may be raised further.

[0041] Drawing 11 - drawing 18 illustrate processing to drawing 3 - drawing 9 . The case where a new user starts a game hereafter from the condition shown in drawing 11 is mentioned as an example, and processing of the network game system of this invention is explained further.

[0042] As for drawing 11 , ID shows the situation that the player data of 1-3 are recorded to store player table 3a and store player table 4a.

[0043] Drawing 12 shows the user 50 with the new pocket site server 5 the situation when publishing a password (refer to drawing 3 and drawing 4). A user 50 is the member of the website which the pocket site server 5 is managing, and makes demands for password issue on the pocket site server 5 from a cellular phone 6. The pocket site server 5 which received the demand publishes a password, and makes it display on a cellular phone 6.

[0044] Drawing 13 and drawing 14 show the game machine 1 in case a user 50 plays for the first time with a game machine 1, and each server's situation (refer to drawing 5 and drawing 6). In drawing 13 , a user throws in coin and inserts the intact (ID is not recorded yet) entry card 2 in a game machine 1. A game machine 1 detects that ID is not recorded on the entry card 2 yet, and transmits ID issue demand to the store server 3. The store server 3 creates the player data containing the ID, and transmits to a game machine 1 while he publishes ID. In drawing 14 , the player data which the user customized are transmitted to the store server 3 from a game machine 1. The store server 3 attaches the date to the data, and records on store player server 3a. In this drawing, the player data of ID=4 are newly added as a user's 50 player data. In addition, the column of a password serves as NULL as an invalid mark at this time. The store server 3 transmits this player data to the pin center,large server 4. The pin center,large server 4 records the received player data on pin center,large player table 4a. Next, the pin center,large server 4 transmits the date to the store server 3. The store server 3 corrects the date of the player data of ID=4 currently recorded on store player table 3a.

[0045] Drawing 15 and drawing 16 show the game machine 1 and the situation of each server, when a user 50 registers a password (refer to drawing 8 and drawing 9). In drawing 15 , a user 50 enters a password while inserting

the entry card 2 in a game machine 1. ID read in the password and the entry card 2 is transmitted to the pin center,large server 4 via the store server 3 from a game machine 1. The pin center,large server 4 searches the player data with which this ID is contained. If the column of the password of the corresponding player data is NULL, a password will be recorded there (this drawing ID= 4 player data). In drawing 16 , as for the pin center,large server 4, registration of a password notifies the store server 3 of a success or failure. If it is a success, the store server 3 will record a password on the player data of ID=4 of store player table 3a. As for the store player server 3, registration of a password notifies a success or failure to a game machine 1 at a game machine 1.

[0046] Drawing 17 and drawing 18 show the game machine 1 and each server's situation, when a user 50 plays 2nd henceforth (refer to drawing 5 and drawing 7). In drawing 17 , a user 50 puts coin into a game machine 1, and inserts an entry card. If password registration has already finished, it is not necessary to enter a password. A game machine 1 reads ID in the entry card 2 (this drawing ID= 4), and requires the player data containing the ID of the store server 3. If the store server 3 has player data applicable to store player table 3a and there is about the player data, he will transmit ID to the pin center,large server 4, and will demand player data. [no] The pin center,large server 4 reads the corresponding player data (ID=4) from pin center,large player table 4a. In drawing 18 , the pin center,large server 4 transmits player data etc. according to the demand advanced by drawing 17 by the store server 3. That is, when player data are received from the store server 3, the date of player data which received is compared with the date of the player data with which pin center,large server 4a corresponds, and the sign of "O.K." will be transmitted if the player data which received the player data when the pin center,large server 4a was newer are newer. When ID is received from the store server 3, the player data with which pin center,large server 4a corresponds are transmitted. In addition, the sign of "BAD" is transmitted when a certain error of there being no player data applicable to pin center,large server 4a occurs. The store server 3 transmits the player data of store player table 3a to a game machine 1, when "O.K." is received. When player data are received, while recording the player data on store player table 3a (updating), it transmits to a game machine 1.

[0047] As mentioned above, according to this operation gestalt, a member number for processing of step S423 and step S324 (drawing 9) to receive ID for playing a game using player data with a game machine 1 and service of the website which the pocket site server 5 manages is matched with a password. Since a password is published by the pocket site server 5 when a user demands issue from a cellular phone 6 (step S502 of drawing 3), it is not necessary to print and manufacture and sell it on the entry card 2. Moreover, since a password is displayed on the screen of a cellular phone 6 (step S603 of drawing 3), it does not have a possibility that it may be stolen by other users as compared with the case where it displays on a game machine 1. Furthermore, if it inputs into a game machine 1 once at step S122 (drawing 8), since ID and a member number are matched, this password is only used inside a game system, and it is not necessary to enter it from a game machine 1 and a cellular phone 6 any more. Therefore, the network game system which can realize the high user authentication system of security cheaply can be offered.

[0048] In addition, this invention is not limited to the above operation gestalt, but may be carried out with various gestalten. For example, the store server 3, the pin center,large server 4 and the pin center,large server 4, and the pocket site server 5 may unify, and may unify these three. On the contrary, each server may be distributed further and each server's burden may be mitigated. A game machine 1 may perform issue of ID, and generation of the player data of an initial state. The function as a junction monitor of a game advance situation may be included in the store server 3, and the function which carries out unitary management of the game advance situation, and the function to transmit a game advance situation to each store server 3 may be included in the pin center,large server 4. The function to check whether the received password exists to the pocket site server 5 may be included in the pin center,large server 4. The entry card 2 is not restricted to the thing using the MAG and IC, but just records ID. ID may be recorded on the entry card from the beginning. A password is not restricted to the thing based on a member number, but may be directly generated from cellular phone ID that what is necessary is just what specifies the user who receives service at an individual terminal. Moreover, even if it is not what enciphered the information which specifies a user, if a password does not have the information which specifies a user from a password by other users recognized, it is good. For example, you may enable it to refer to a password from a member number by matching the password with a member number and recording it, using as a password the character string which made it generate at random.

[0049] The network system of this invention is not limited to what uses a game machine or a game terminal as a common terminal, but can be applied to various applications. For example, when the training machine of sport crab is set up as a common terminal, the user data (for example, movement time amount, consumption energy) based on the contents of use of the training machine are recorded on a database, and this invention can be applied also when making the user data available from individual terminals, such as a cellular phone. In this case, a use gestalt which it considers as reference of selection of the contents of a meal, or the contents of a meal actually took in with reference to movement time amount etc. for example, on the individual terminal are transmit [gestalt] from an individual terminal, and a database is update [gestalt], and makes user's individual's everyday life reflect in the decision of the training menu in sport crab by that cause is possible for use of the user data from an individual terminal.

[Translation done.]

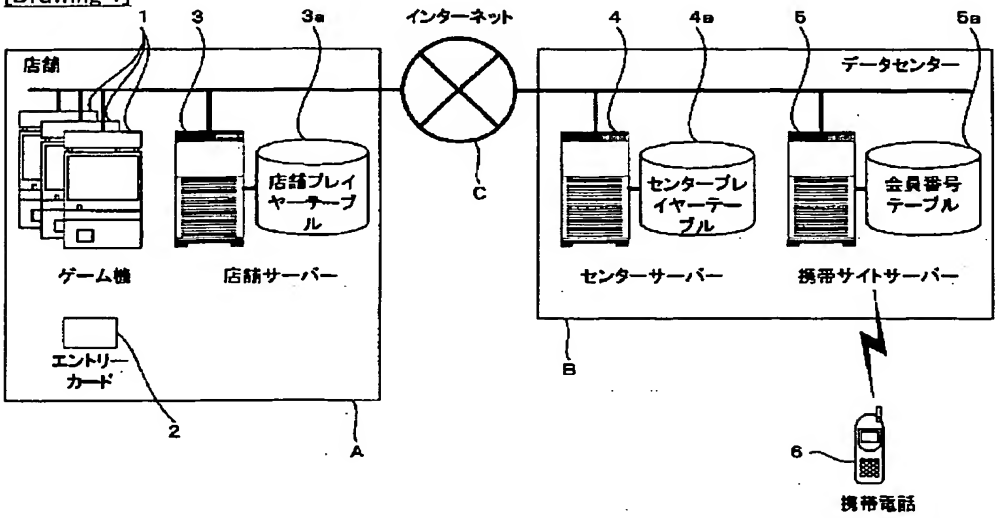
DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] Drawing showing the network game structure of a system concerning 1 operation gestalt of this invention.
[Drawing 2] Drawing showing the contents of the data recorded on the storage means of the network game system of drawing 1 .
[Drawing 3] The flow chart which shows the procedure of the password issue processing which a cellular phone and a pocket site server perform.
[Drawing 4] Drawing showing the example of the screen of the cellular phone in processing of drawing 3 .
[Drawing 5] The flow chart which shows the procedure of processing from the game initiation which a game machine performs to termination.
[Drawing 6] The flow chart which shows the procedure of the first time registration processing which a store server and a pin center,large server perform.
[Drawing 7] The flow chart which shows the procedure of the data transmitting processing which a store server and a pin center,large server perform when there is a demand of data transmission from a game machine.
[Drawing 8] The flow chart which shows the procedure of the password registration processing which a game machine performs.
[Drawing 9] The flow chart which shows the procedure of the password registration processing which the store server 3 and the pin center,large server 4 perform.
[Drawing 10] The flow chart which shows the procedure of the data transmitting processing which a pin center,large server and a pocket site server perform when there is a demand of transmission of data from a cellular phone.
[Drawing 11] Drawing showing the example of 1 situation of a game system.
[Drawing 12] Drawing showing the example of a situation when publishing a password.
[Drawing 13] Drawing showing the example of a situation in case a user plays for the first time.
[Drawing 14] Drawing showing the example of a situation in case a user plays for the first time.
[Drawing 15] Drawing showing the example of a situation in case a user registers a password.
[Drawing 16] Drawing showing the example of a situation in case a user registers a password.
[Drawing 17] Drawing showing the example of a situation in case a user plays 2nd henceforth.
[Drawing 18] Drawing showing the example of a situation in case a user plays 2nd henceforth.
[Description of Notations]
1 Game Machine
2 Entry Card
3 Store Server
3a Store player table
4 Pin Center,large Server
4a Pin center,large player table
5 Pocket Site Server
5a Member number table
6 Cellular Phone

[Translation done.]

DRAWINGS

[Drawing 1]



[Drawing 2]

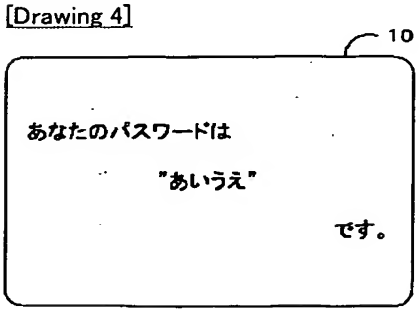
(a)

携帯ID	会員番号
645	311
356	312
238	313

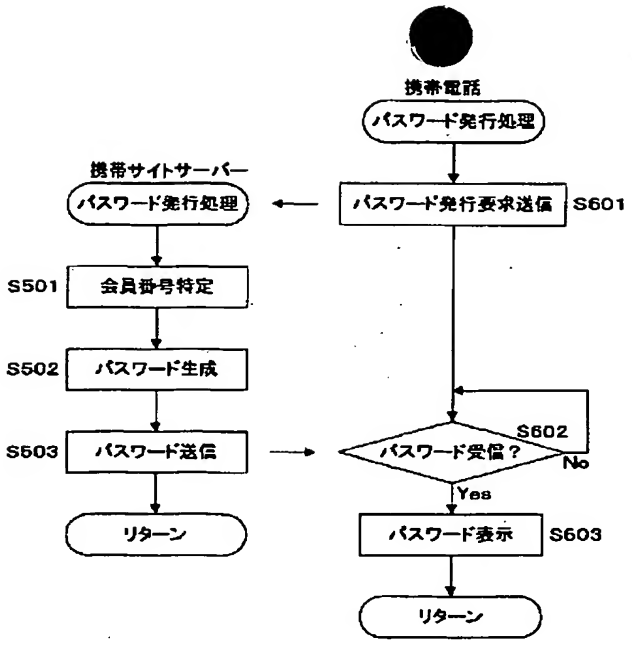
(b)

ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大巻巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…

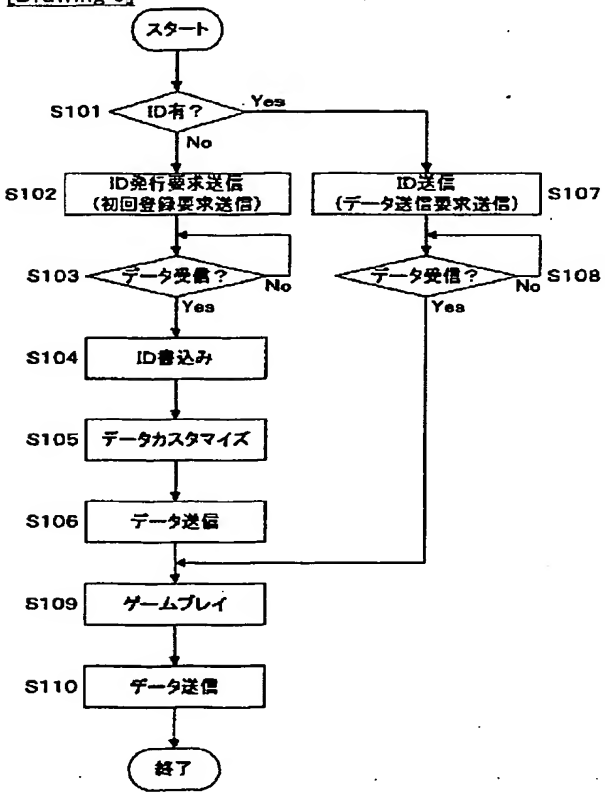
[Drawing 4]



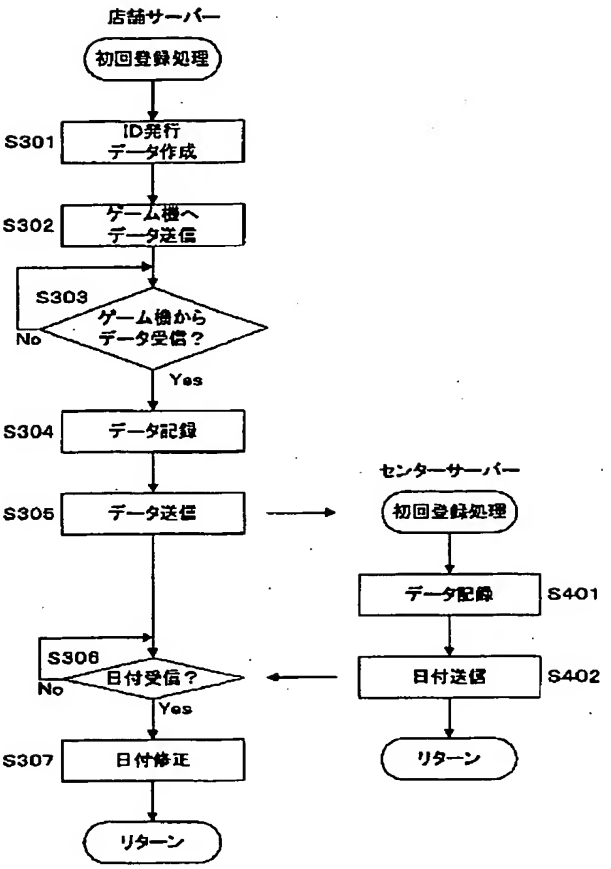
[Drawing 3]



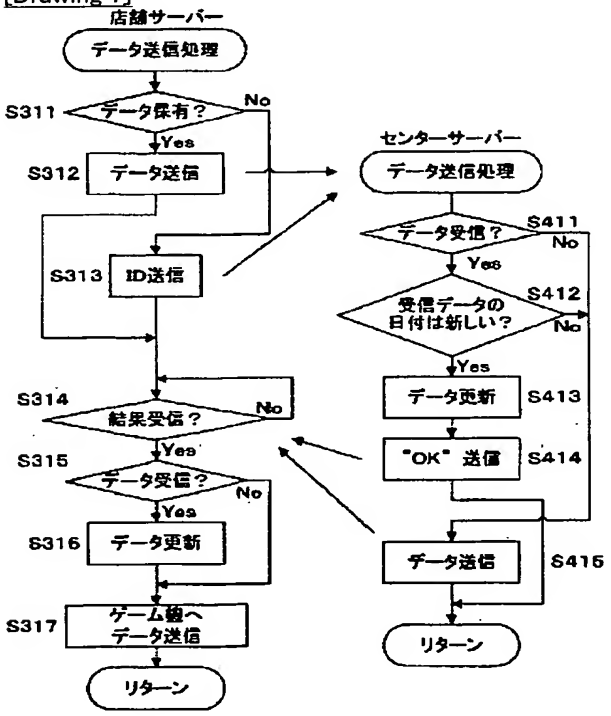
[Drawing 5]



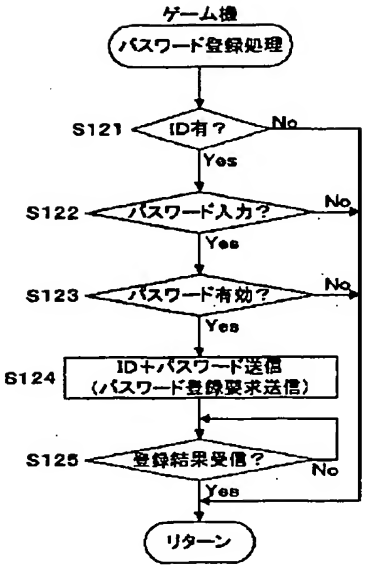
[Drawing 6]



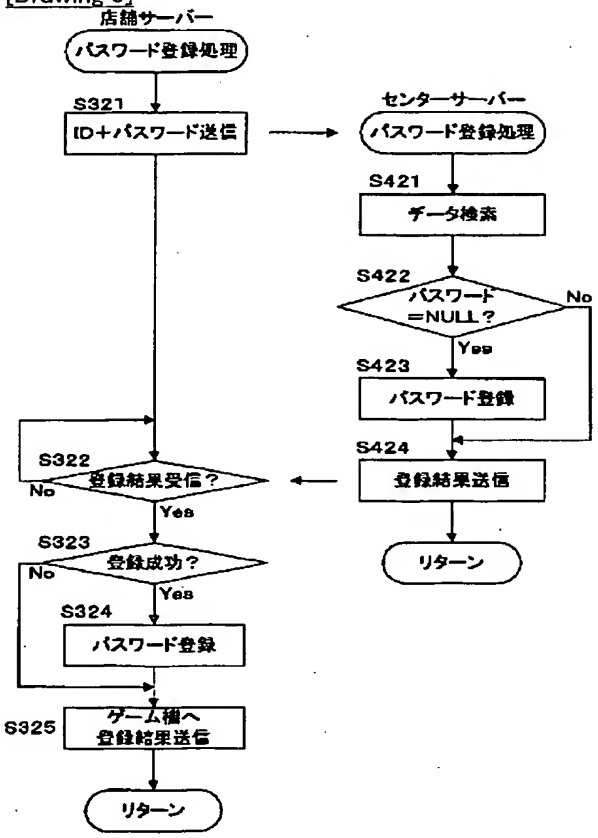
[Drawing 7]



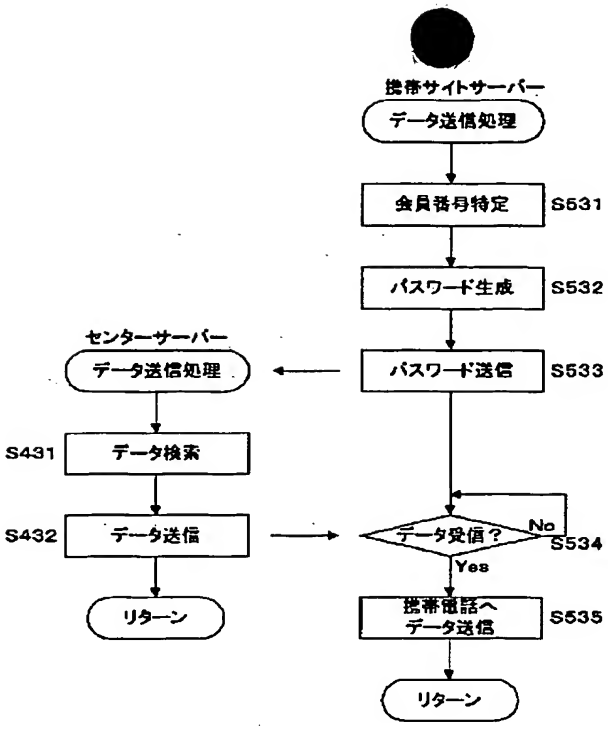
[Drawing 8]



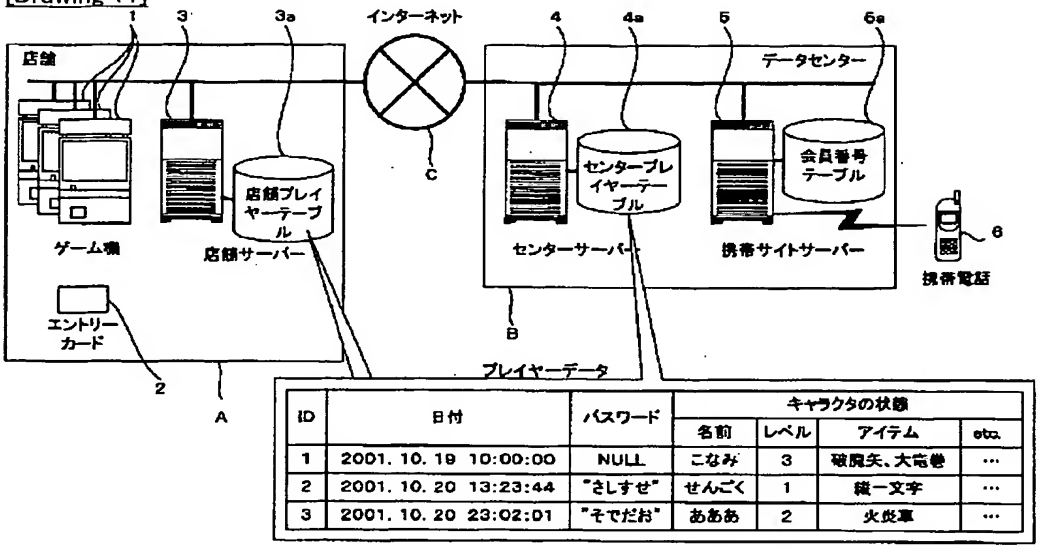
[Drawing 9]



[Drawing 10]

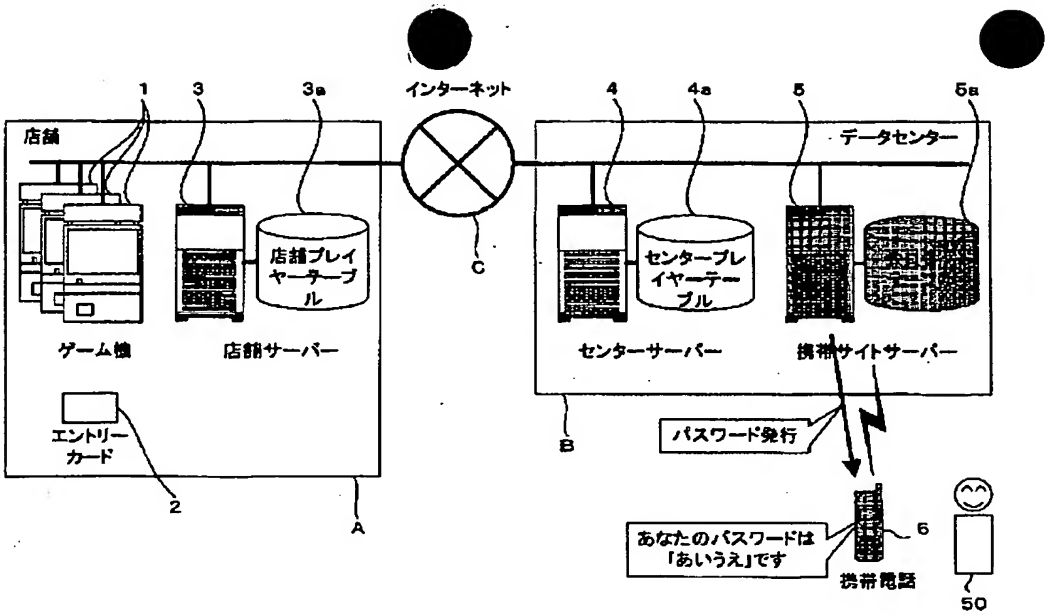


[Drawing 11]

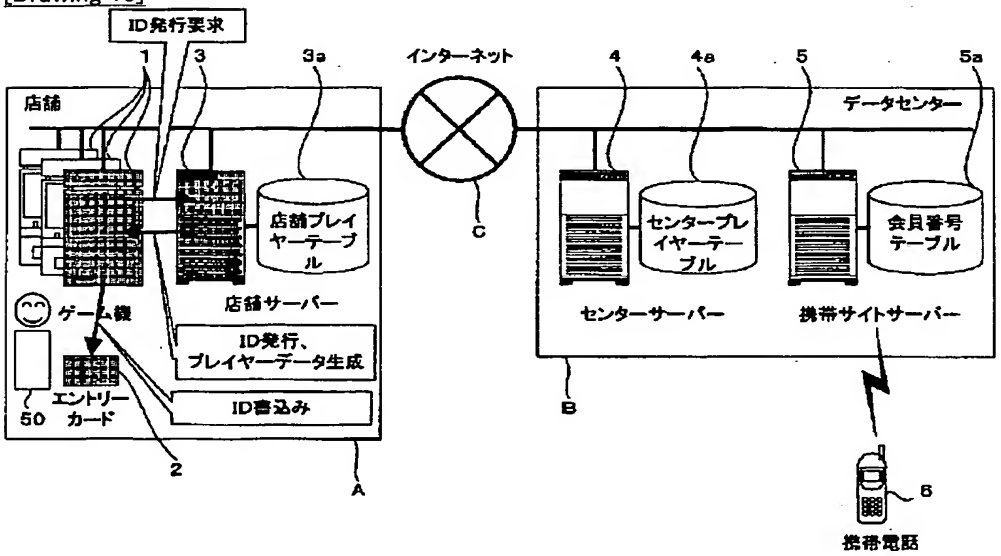


ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大弓巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…

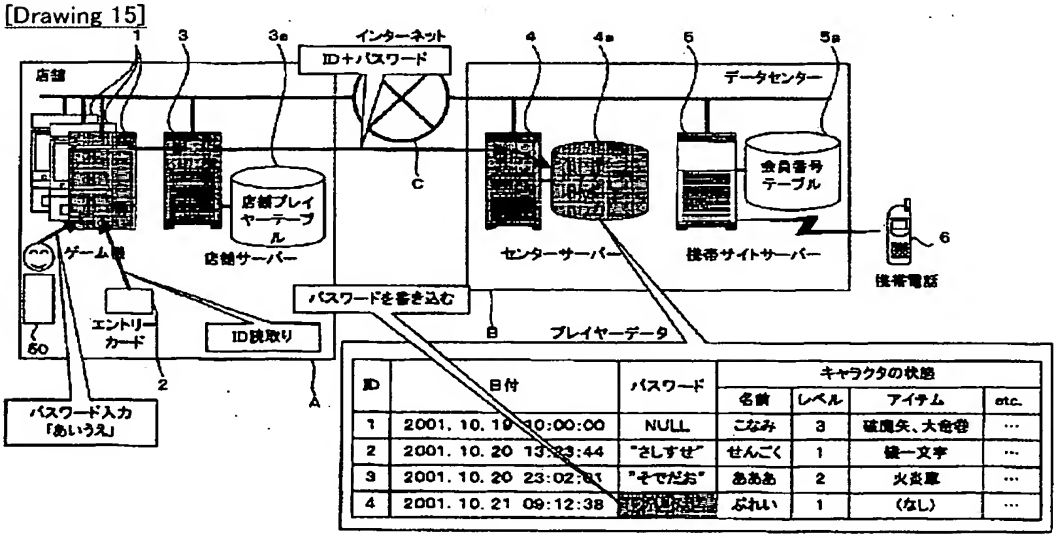
[Drawing 12]



[Drawing 13]

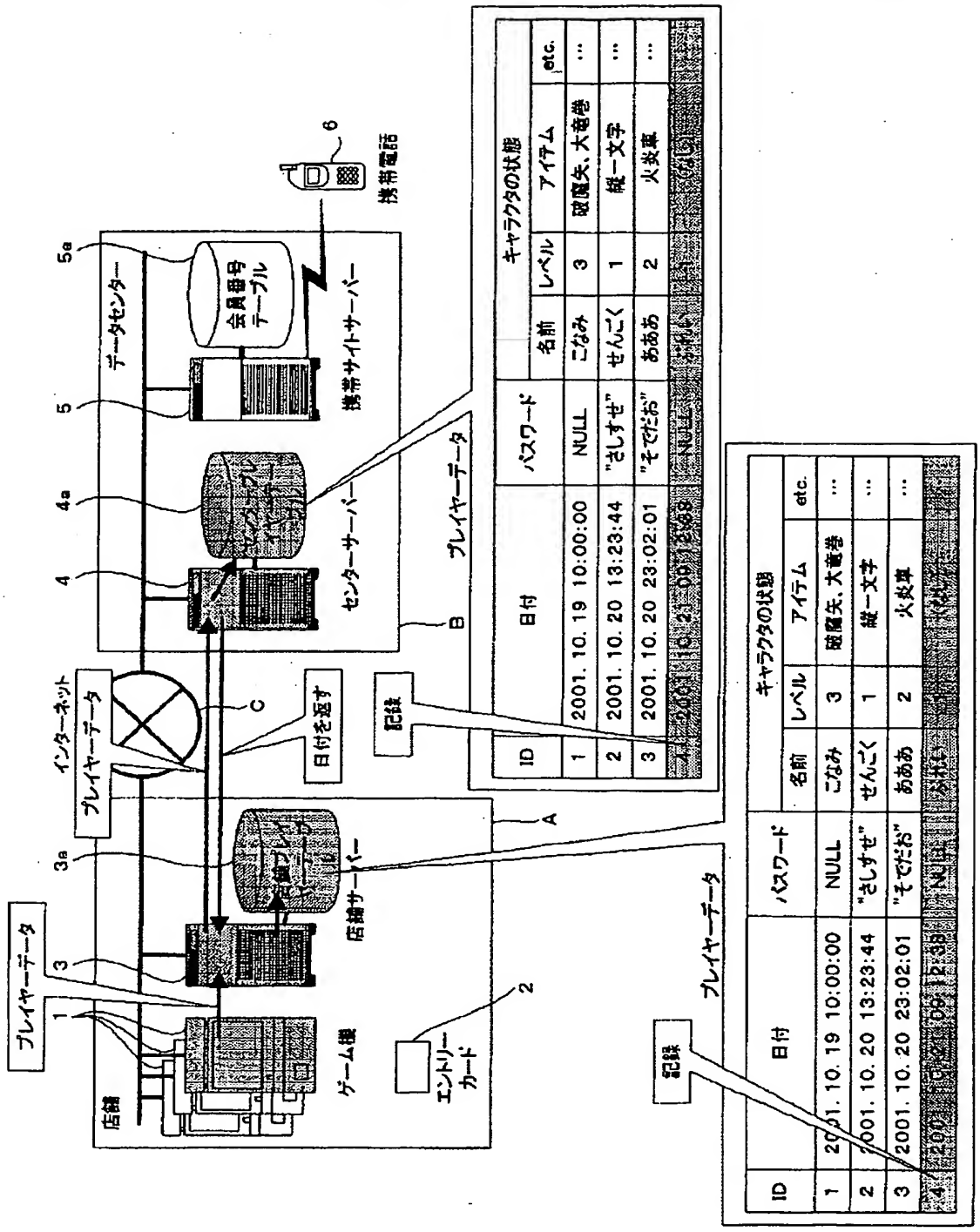


[Drawing 15]

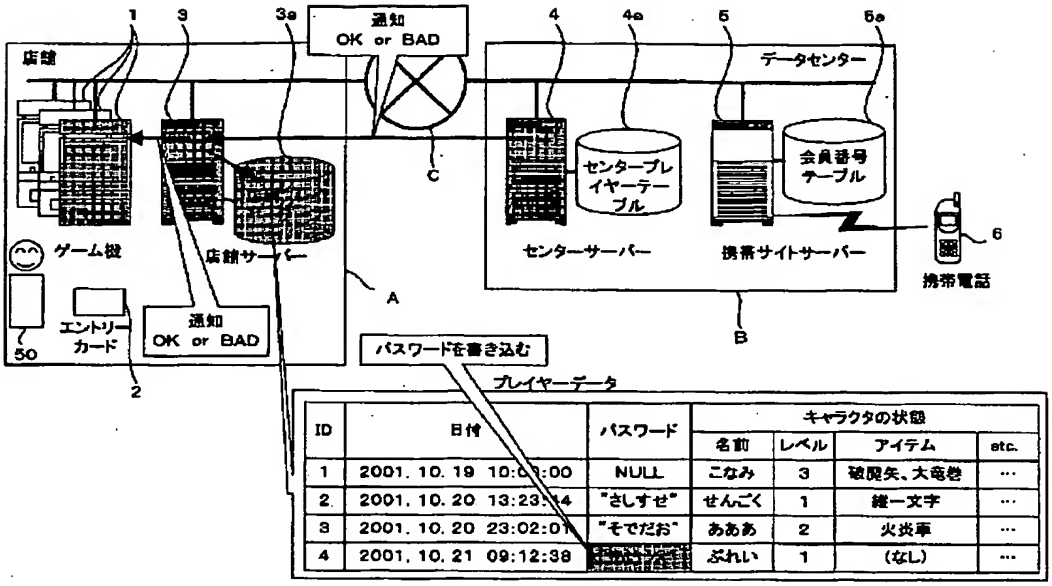


ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大命谷	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	破一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…
4	2001. 10. 21 09:12:38	[illegible]	ぶれい	1	(なし)	…

[Drawing 14]

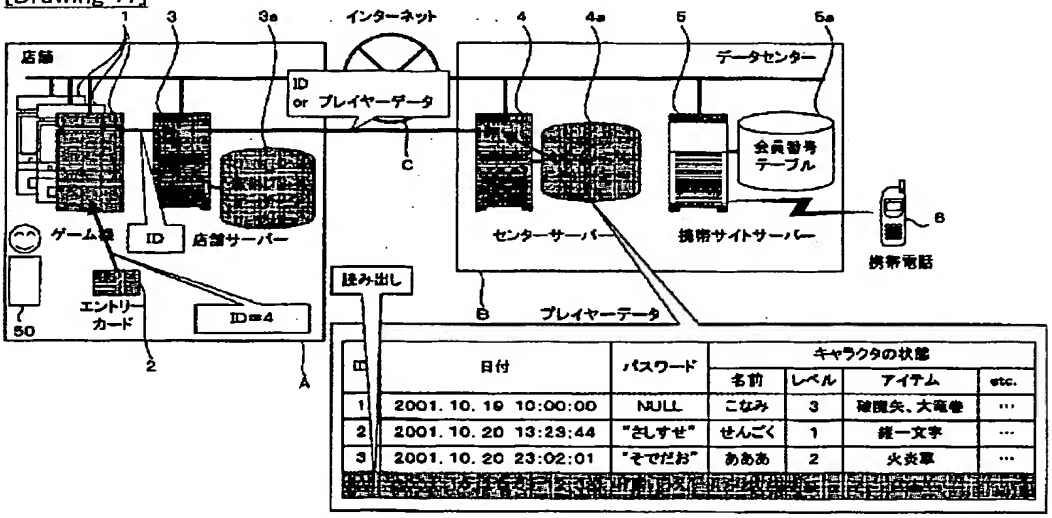

店舗
ゲーム機
エントリーカード
プレイヤーデータ
店舗サーバー
インターネット
センターサーバー
携帯サイトサーバー
データセンター
会員番号テーブル
携帯電話
日付を返す
記録
A
B
C
1
2
3
4
5
6
3a
4a
5a
ID
日付
パスワード
キャラクタの状態
名前
レベル
アイテム
etc.
こなみ
せんごく
ああああ
破魔矢、大竜巻
縦一文字
火炎車
NULL
"そしず"
"そでだお"

[Drawing 16]



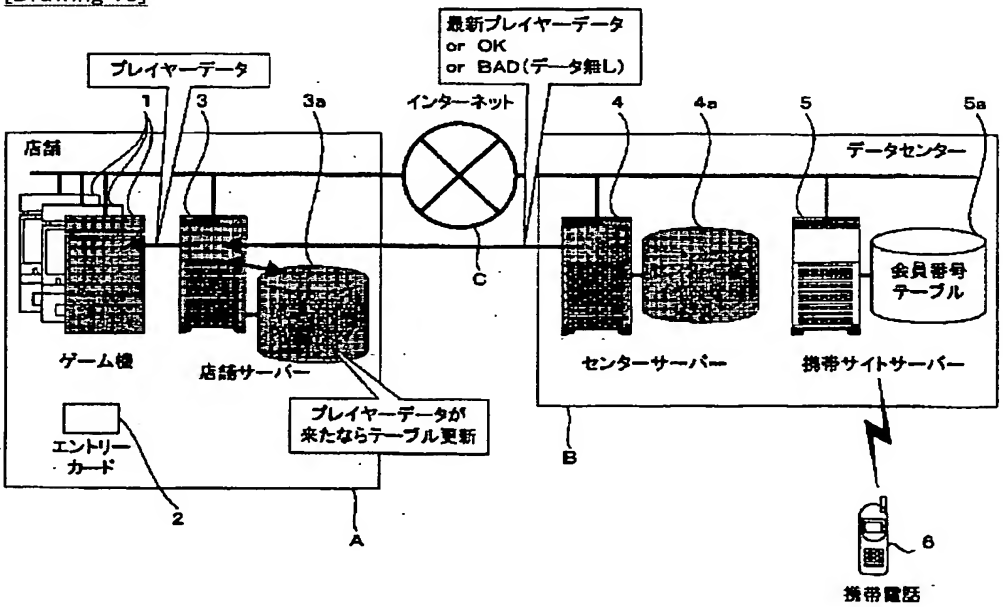
ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破関矢、大竜巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	維一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…
4	2001. 10. 21 09:12:38		ぶれい	1	(なし)	…

[Drawing 17]



ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破関矢、大竜巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	維一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…

[Drawing 18]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－157237
（P2003－157237A）
(43)公開日　平成15年５月30日(2003.5.30)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	２Ｃ００１
Ｈ０４Ｑ　7/38		Ａ６３Ｆ　13/12	Ｃ	５Ｂ０８５
// Ａ６３Ｆ　13/12		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｋ０６７

審査請求　有　　請求項の数11　ＯＬ　（全 19 頁）

(21)出願番号　特願2001－355349(P2001－355349)

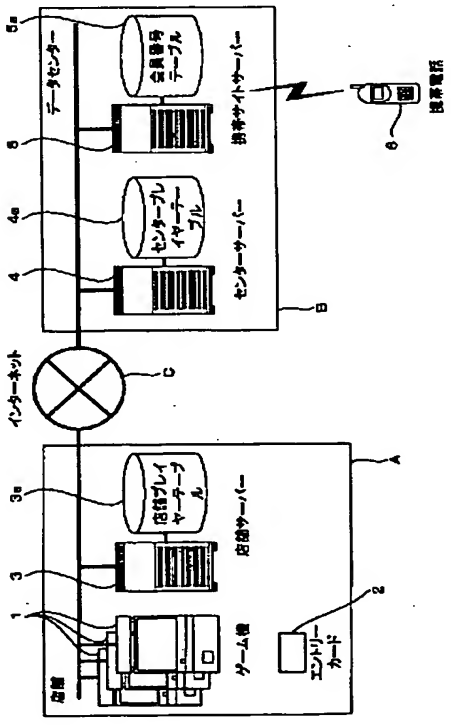
(22)出願日　平成13年11月20日(2001.11.20)

(71)出願人　000105637
コナミ株式会社
東京都千代田区丸の内２丁目４番１号
(72)発明者　高橋　一也
東京都港区虎ノ門四丁目３番１号　コナミ株式会社内
(72)発明者　菅野　啓
東京都港区虎ノ門四丁目３番１号　コナミ株式会社内
(74)代理人　100099645
弁理士　山本　晃司　（外２名）

最終頁に続く

(54)【発明の名称】　ネットワークシステム

(57)【要約】
【課題】　携帯電話等の個人端末からユーザデータを利用可能とするために必要な情報の発行や入力に関する安全性を高め、かつその情報を低コストでユーザに提供する。
【解決手段】　一般端末１を利用するユーザ識別情報とそのユーザのユーザデータとを対応付けて記憶手段４に記憶する。個人端末６からパスワードの発行要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるユーザ固有のアクセス識別情報を取得し、そのアクセス識別情報に対して一義的に定められたパスワードを発行し、そのパスワードを個人端末６に通知する。一般端末１にてパスワードとユーザ識別情報とが相互に関連付けて入力された場合、その入力されたユーザ識別情報に対応して記憶手段４が記憶するユーザデータを対象として、入力されたパスワードに対応するアクセス識別情報との関連付けを設定する。



1

【特許請求の範囲】

【請求項１】　不特定のユーザによる利用を前提として設置された一般端末を複数のユーザのそれぞれが利用した内容に基づいてユーザ毎に生成されるユーザデータを、各ユーザを特定するためのユーザ識別情報と対応付けて記憶する記憶手段と、

各ユーザが個人的に使用する個人端末からパスワードの発行要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるユーザ固有のアクセス識別情報を取得し、そのアクセス識別情報に対して一義的に定められたパスワードを発行するパスワード管理手段と、

発行されたパスワードを前記個人端末に通知するパスワード通知手段と、

前記一般端末にて前記パスワードと前記ユーザ識別情報とが相互に関連付けて入力された場合、その入力されたパスワードとユーザ識別情報とを一般端末から受け取り、その受け取ったユーザ識別情報に対応して前記記憶手段が記憶する前記ユーザデータを対象として、受け取ったパスワードに対応するアクセス識別情報との関連付けを設定する関連付け設定手段と、を備えたことを特徴とするネットワークシステム。

【請求項２】　前記関連付け設定手段は、前記ユーザ識別情報又はそのユーザ識別情報に対応するユーザデータと前記パスワードとを対応付けて記録することにより、前記ユーザデータと前記アクセス識別情報との関連付けを設定することを特徴とする請求項１に記載のネットワークシステム。

【請求項３】　前記個人端末から前記ユーザデータに関する所定の要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるアクセス識別情報に対応するパスワードを前記パスワード管理手段が特定し、

その特定されたパスワードに対応するユーザデータを特定するユーザデータ特定手段をさらに備えたことを特徴とする請求項２に記載のネットワークシステム。

【請求項４】　前記パスワード管理手段は、前記アクセス識別情報に対して所定の処理を実行して前記パスワードを生成し、同一のアクセス識別情報に対しては同一のパスワードが生成されるように前記所定の処理が構成されていることを特徴とする請求項３に記載のネットワークシステム。

【請求項５】　前記記憶手段に記録されたユーザデータのうち、前記関連付けが設定されているユーザデータを抽出するユーザデータ抽出手段と、

抽出されたユーザデータと対応付けて記録されたパスワードと、前記アクセス識別情報との対応関係とを利用して、前記抽出されたユーザデータに対応するアクセス識別情報を特定するアクセス識別情報特定手段と、

特定されたアクセス識別情報に対応する個人端末へ所定の情報を配信する配信制御手段とを備えることを特徴とする請求項２～４のいずれか１項に記載のネットワークシステム。

2

【請求項６】　前記関連付けが既に設定されているユーザデータに関しての前記関連付け設定手段による前記関連付けの再設定を禁止する禁止手段を備えていることを特徴とする請求項１～５のいずれか１項に記載のネットワークシステム。

【請求項７】　前記一般端末に設けられ、所定の記録媒体に対する前記ユーザ識別情報の書き込みと、書き込まれたユーザ識別情報の読み込みとを行う読み書き手段と、

前記記録媒体に前記ユーザ識別情報が記録されていないときに、ユーザ識別情報を発行する発行手段と、

発行されたユーザ識別情報を所定の初期ユーザデータと対応付けて前記記録手段に記録する初期データ記録手段と、を備え、

発行されたユーザ識別情報が前記読み書き手段を介して前記記録媒体に書き込まれることを特徴とする請求項１～６のいずれか１項に記載のネットワーシステム。

【請求項８】　不特定のユーザによる利用を前提として設置された一般端末を複数のユーザのそれぞれが利用した内容に基づいてユーザ毎に生成されるユーザデータを、各ユーザを特定するためのユーザ識別情報と対応付けて記録したデータベースを保有し、前記ユーザ認識情報を伴った送信要求に応答してその認識情報に対応したユーザデータを送信するユーザデータ管理装置と、

会員が個人的に使用する個人端末とネットワークを介して接続され、前記個人端末からのアクセス識別情報を伴ったアクセスに対して所定のサービスを提供するネットワークサービス提供装置と、を具備し、

前記ネットワークサービス提供装置は、

前記個人端末から、パスワードの発行要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるアクセス識別情報に対して一義的なパスワードを発行するパスワード管理手段と、

発行されたパスワードを前記個人端末に通知するパスワード通知手段と、

前記個人端末からのユーザデータ利用要求に応答して、その個人端末を使用する会員のアクセス識別情報に対応するパスワードを前記ユーザデータ管理装置に提供するパスワード提供手段と、を具備し、

前記ユーザデータ管理装置は、

前記一般端末にて前記ユーザ識別情報と前記パスワードとが相互に関連付けて入力された場合、その入力されたユーザ識別情報とパスワードとを一般端末側から受け取り、その受け取ったユーザ識別情報に対応するユーザデータと前記パスワードとの関連付けを前記データベース上で設定する関連付け設定手段と、

前記ネットワークサービス提供装置から前記パスワードが提供されたとき、その提供されたパスワードに関連付けられたユーザデータを特定し、その特定されたユーザ

データに関する前記個人端末上での利用を可能とするデータ利用制御手段と、を備えたことを特徴とするネットワークシステム。

【請求項９】　前記個人端末からのアクセスに応答してその個人端末に固有の端末識別情報を特定し、その特定された端末識別情報を添えてアクセス内容を通知する所定の通信処理システムを介して前記ネットワークサービス提供装置に接続される特定個人端末を前記個人端末が含んでおり、

前記ネットワークサービス提供装置は、前記端末識別情報と前記ネットワークサービス提供装置からのサービス提供範囲で通用する会員毎の会員識別情報とを対応付けた会員情報テーブルを保有し、前記特定個人端末からアクセスがあった場合には、前記端末識別情報を前記アクセス識別情報として取得し、前記会員情報テーブルを参照して、その取得されたアクセス識別情報に対応する会員識別情報を特定する会員情報管理手段を具備し、

前記パスワード管理手段は、前記会員識別情報に基づいて前記パスワードを発行することを特徴とする請求項８に記載のネットワークシステム。

【請求項１０】　前記一般端末には、所定の記録媒体に対する前記ユーザ識別情報の書き込みと、書き込まれたユーザ識別情報の読み込みとを行う読み書き手段と、前記記録媒体に有効なユーザ識別情報が記録されていない場合にユーザ識別情報の発行要求を出力する発行要求手段とが設けられ、

前記ネットワークシステムには、前記発行要求手段からの要求に応じて新たなユーザ識別情報を発行して前記一般端末及び前記ユーザデータ管理装置に提供するユーザ識別情報管理装置が設けられ、

前記ユーザデータ管理装置は、前記新たなユーザ識別情報を前記ユーザ識別情報管理装置から取得し、その取得されたユーザ識別情報を所定の初期ユーザデータと対応付けて前記データベースに記録し、

前記一般端末の前記読み書き手段は、前記ユーザ識別情報管理装置から前記新たなユーザ識別情報を取得した場合に、そのユーザ識別情報を前記記録媒体に記録する、ことを特徴とする請求項８又は９に記載のネットワークシステム。

【請求項１１】　前記一般端末が複数の店舗のそれぞれに設置される一方で、前記ユーザデータ管理装置は前記複数の店舗の一般端末に共通して設置され、前記ユーザ識別情報管理装置は、各店舗の一般端末と前記ユーザデータ管理装置との間でかつ店舗毎に設けられていることを特徴とする請求項１０に記載のネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを介して一般端末や個人端末を結び付けることが可能なネットワークシステムに関する。

【０００２】

【従来の技術】ユーザがゲームセンターのゲーム端末にてプレイした内容に基づいてゲームデータを作成し、そのゲームデータを所定のサーバーに保存する一方で、そのサーバーにユーザが携帯電話等の個人端末からアクセスしてゲームデータを利用可能とするゲームシステムが知られている。

【０００３】このようなゲームシステムにおいては、個人端末からアクセスしたユーザがどのゲームデータと対応しているのかを特定する必要がある。こうした対応関係を特定する方法としては、ゲーム端末にてパスワードを生成してゲームデータとともにサーバーに送信し、これを受けたサーバーがパスワードとゲームデータとを対応付けて保存する一方で、そのパスワードをゲーム機の画面に表示し、ユーザが個人端末からサーバーにアクセスする際にそのパスワードを入力させ、その入力されたパスワードを利用してゲームデータを特定する方法が考えられる。

【０００４】その他の方法としては、予めユニークなＩＤが記録され、かつ、そのＩＤが印刷されたカードを予め用意し、このカードをゲーム端末のユーザに対して販売する方法がある。ユーザはカードを購入し、そのカードをゲーム機に挿入してゲームをプレイする。ゲーム機はカードに記録されたＩＤを読込み、そのＩＤをゲームデータとともにサーバーに送信する。サーバーは送信されたＩＤとゲームデータとを対応付けて保存する。ユーザは携帯電話等の個人端末からサーバーにアクセスし、カードに印刷されたＩＤを入力することにより、自己のゲームデータにアクセスすることができる。

【０００５】

【発明が解決しようとする課題】しかしながら、ゲームセンターのように不特定多数のユーザが集まっている場所に設置された一般端末の画面にパスワードを表示する場合には、他人にパスワードが盗まれるおそれがある。また、上述のカードを使用する方法では、ユーザの手に渡る前のカードに予めユニークなＩＤを記録し、かつそれと同一のＩＤをカードに印刷しておく必要がある。従って、カードの製造や管理に手間がかかり、カードの販売価格を押し上げる要因となる。

【０００６】そこで、本発明は、一般端末の利用内容に基づいて生成されてユーザ識別情報と対応付けて記録されるユーザデータを、一般端末とは異なる携帯電話等の個人端末から利用可能とするために必要な情報の発行や入力に際しての安全性が高く、かつそのような情報を低コストでユーザに提供することが可能なネットワークシステムを提供することを目的とする。

【０００７】

【課題を解決するための手段】以下、本発明について説明する。なお、本発明の理解を容易にするために添付図

面の参照符号を括弧書きにて付記するが、それにより本発明が図示の形態に限定されるものではない。

【０００８】本発明のネットワークシステムは、不特定のユーザによる利用を前提として設置された一般端末（１）を複数のユーザのそれぞれが利用した内容に基づいてユーザ毎に生成されるユーザデータを、各ユーザを特定するためのユーザ識別情報と対応付けて記憶する記憶手段（４）と、各ユーザが個人的に使用する個人端末（６）からパスワードの発行要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるユーザ固有のアクセス識別情報を取得し、そのアクセス識別情報に対して一義的に定められたパスワードを発行するパスワード管理手段（５）と、発行されたパスワードを前記個人端末に通知するパスワード通知手段（５）と、前記一般端末にて前記パスワードと前記ユーザ識別情報とが相互に関連付けて入力された場合、その入力されたパスワードとユーザ識別情報とを一般端末から受け取り、その受け取ったユーザ識別情報に対応して前記記憶手段が記憶する前記ユーザデータを対象として、受け取ったパスワードに対応するアクセス識別情報との関連付けを設定する関連付け設定手段（４）と、を備えることにより、上述した課題を解決する。

【０００９】本発明のネットワークシステムによれば、ユーザ識別情報に対応付けて記録されているユーザデータを、個人端末から利用可能とするために必要な情報としてパスワードが機能する。すなわち、パスワードを媒介として、アクセス識別情報とユーザデータとが関連付けられる。パスワードはネットワークシステムが適宜に発行するため、予めユニークなＩＤが記録され、かつ、そのＩＤが印刷されたカードをユーザに配布するような手間がかからず、パスワードをユーザに低コストで提供できる。パスワードが一般端末ではなく、ユーザの個人使用に係る個人端末に表示される。従って、不特定多数のユーザが利用する一般端末の画面上にパスワードを表示する場合と比較して、他のユーザにパスワードを盗まれる可能性は遙かに低く、それだけパスワードの発行に関する安全性が高い。パスワードをユーザ識別情報と関連付けて一般端末に入力すると、その入力したユーザ識別情報に対応するユーザデータを対象として、パスワードに対応するアクセス識別情報の関連付けが設定されるので、それ以降、パスワードはアクセス識別情報とユーザデータとを対応付ける媒介としてシステムの内部で用いられるだけである。あるいは、関連付けを設定する際に、パスワードを媒介として、ユーザデータとアクセス識別情報との対応関係を判別し、その判別された対応関係を特定するためのパスワード以外の情報を記憶手段に記録しておけば、アクセス識別情報からそのパスワード以外の情報を媒介としてユーザデータを割り出せるようになり、パスワードを使用する必要がなくなる。このため、再度、一般端末や個人端末からパスワードを入力する必要はない。従って、パスワードの入力に関しても安全性が高い。

【００１０】なお、一般端末は各種のコンピュータ機器を含む。さらには、ゲームセンターに設置されるアーケードゲーム機、インターネットカフェに設置されるパーソナルコンピュータ、スポーツクラブに設置されるトレーニングマシンのように、商業施設に設置され、不特定多数のユーザが利用可能な機器を一般端末とした場合に本発明は好適である。但し、一般端末の設置目的の営利、非営利は問わない。個人端末は、ネットワーク接続機能を有する各種のコンピュータ機器を含む。さらには、携帯電話、ＰＤＡ、携帯型ゲーム機のような個人的な使用を前提として構成されている情報機器が個人端末として使用される。家庭内に設置されるパーソナルコンピュータやビデオゲーム装置を個人端末として使用することもできる。但し、個人端末がユーザの所有に係るか否かは問わない。事実上ユーザが個人的に使用するコンピュータ機器であれば個人端末として使用可能である。

【００１１】パスワード管理手段は、所定のアルゴリズムによって一義的なパスワードを生成するものでもよいし、予め定められたパスワード群からいずれか一つのパスワードを抽出してアクセス識別情報と対応付けることにより、アクセス識別情報に対して一義的なパスワードを発行するものでもよい。パスワード通知手段は、文字列を利用してパスワードを通知するものでもよいし、音声信号によりパスワードを通知するものでもよい。

【００１２】前記関連付け設定手段は、前記ユーザ識別情報又はそのユーザ識別情報に対応するユーザデータと、受け取ったパスワードとを対応付けて記録することにより、前記ユーザデータとアクセス識別情報との関連付けを設定することができる。この場合には関連付けが容易に設定できる。

【００１３】但し、関連付け設定手段は、受け取ったパスワードに対応してさらに一義的に定められる他の情報をユーザデータと対応付けて記録してもよい。パスワードに対して一義的に定められる情報は、例えばパスワードを所定のアルゴリズムで処理することによって生成されてもよい。ユーザ識別情報又はユーザデータと対応付けて記録すべき情報の候補を予め幾つか用意し、受け取ったパスワードに対していずれかの候補を一義的に割り当てるような方法によっても、パスワードから一義的に定められた情報を生成することができる。

【００１４】関連付け設定手段がパスワードをユーザデータと対応付けて記録する場合にはさらに次のような態様が可能である。

【００１５】前記個人端末から前記ユーザデータに関する所定の要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるアクセス識別情報に対応するパスワードを前記パスワード管理手段が特定し、その特定されたパスワードに対応するユーザデータを特定するユ

ーザデータ特定手段（４）をさらに備えるようにしてもよい。この場合には、パスワード管理手段が、個人端末からのパスワード発行要求に応えてパスワードを発行する手段、及び、パスワード発行済の個人端末からパスワードを媒介としてユーザデータを特定するアクセスがあったときにアクセス識別情報からパスワードを特定する手段として兼用される。これにより、パスワード管理が一元化され、情報管理の手間が軽減される。

【００１６】前記パスワード管理手段は、前記アクセス識別情報に対して所定の処理を実行して前記パスワードを生成し、同一のアクセス識別情報に対しては同一のパスワードが生成されるように前記所定の処理が構成されてもよい。この場合、パスワードとアクセス識別情報との対応関係を別に記録しなくても、アクセス識別情報から同一のパスワードを取得することができる。従って、記憶手段の記憶容量を節約できる。なお、所定の処理は、アクセス識別情報を暗号化するようなものであってもよいし、パスワードに誤入力防止用のチェックコードを含めてもよい。

【００１７】前記記憶手段に記録されたユーザデータのうち、前記関連付けが設定されているユーザデータを抽出するユーザデータ抽出手段（４）と、抽出されたユーザデータに対応付けて記録された前記パスワードと前記アクセス識別情報との対応関係とを利用して、前記抽出されたユーザデータに対応するアクセス識別情報を特定するアクセス識別情報特定手段（５）と、特定されたアクセス識別情報に対応する個人端末へ所定の情報を配信する配信制御手段（５）とをネットワークシステムがさらに備えてもよい。この場合には、個人端末に通知されたパスワードを一般端末から入力したユーザに対してのみ、所定の情報が配信され、パスワード未発行、又は未入力のユーザにはその情報が配信されない。従って、個人端末からアクセスしてパスワードを取得し、かつそのパスワードを入力する動機付けをユーザに与え、本発明のシステムの利用を促すことができる。

【００１８】本発明のネットワークシステムにおいて、前記関連付けが既に設定されているユーザデータに関しての前記関連付け設定手段による前記関連付けの再設定を禁止する禁止手段（５）を備えてもよい。この場合には、一般端末からパスワードを入力して関連付けが設定されると、その後は同一のユーザ識別情報とパスワードとを関連付けて一般端末に入力しても関連付けが変更されることがない。従って、入力中のパスワードが他人に読み取られたとしても被害がなく、パスワードの入力に関する安全性がさらに高まる。

【００１９】本発明のネットワークシステムにおいては、前記一般端末（１）に設けられ、所定の記録媒体（２）に対する前記ユーザ識別情報の書き込みと書き込まれたユーザ識別情報の読み込みとを行う読み書き手段と、前記記録媒体に前記ユーザ識別情報が記録されていないときに、ユーザ識別情報を発行する発行手段（３）と、発行されたユーザ識別情報を所定の初期ユーザデータと対応付けて前記記録手段に記録する初期データ記録手段（４）と、を備え、発行されたユーザ識別情報が前記読み書き手段を介して前記記録媒体に書き込まれるものとしてもよい。この場合、記録媒体がユーザに渡る前に記録媒体にユニークなＩＤを記録する必要がない。従って、記録媒体を安価に製造できる。また、ユーザが購入してから情報を書き込むため、ユーザに記録媒体を柔軟に運用させることができる。

【００２０】本発明の他のネットワークシステムは、不特定のユーザによる利用を前提として設置された一般端末（１）を複数のユーザのそれぞれが利用した内容に基づいてユーザ毎に生成されるユーザデータを、各ユーザを特定するためのユーザ識別情報と対応付けて記録したデータベース（４ａ）を保有し、前記ユーザ認識情報を伴った送信要求に応答してその認識情報に対応したユーザデータを送信するユーザデータ管理装置（４）と、会員が個人的に使用する個人端末（６）とネットワークを介して接続され、前記個人端末からのアクセス識別情報を伴ったアクセスに対して所定のサービスを提供するネットワークサービス提供装置（５）と、を具備し、前記ネットワークサービス提供装置（５）は、前記個人端末からパスワードの発行要求を伴ったアクセスがあった場合、そのアクセスに伴って通知されるアクセス識別情報に対して一義的なパスワードを発行するパスワード管理手段と、発行されたパスワードを前記個人端末に通知するパスワード通知手段と、前記個人端末からのデータ利用要求に応答して、その個人端末を使用する会員のアクセス識別情報に対応するパスワードを前記ユーザデータ管理装置に提供するパスワード提供手段と、を具備し、前記ユーザデータ管理装置（４）は、前記一般端末にて前記ユーザ識別情報と前記パスワードとが相互に関連付けて入力された場合、その入力されたユーザ識別情報とパスワードとを一般端末側から受け取り、その受け取ったユーザ識別情報に対応するユーザデータと前記パスワードとの関連付けを前記データベース上で設定する関連付け設定手段と、前記ネットワークサービス提供装置から前記パスワードが提供されたとき、その提供されたパスワードに関連付けられたユーザデータを特定し、その特定されたユーザデータに関する前記個人端末上での利用を可能とするデータ利用制御手段と、を備えたことにより、上述した課題を解決する。

【００２１】このネットワークシステムにおいて、ユーザデータ管理装置はユーザの一般端末の利用をサポートし、ネットワークサービス提供装置は会員に対して一般端末の利用に限らず種々のサービスを提供することができる。ユーザデータ管理装置がユーザ識別情報とユーザデータとを対応付けたデータベースを保有するため、ユーザ識別情報を手掛かりとして、ユーザが自己のユーザ

データをユーザデータ管理装置から一般端末に読み込んで利用することができる。ネットワークサービス提供装置は、アクセス識別情報に対応したパスワードを発行して個人端末に通知し、ユーザデータ管理装置はそのパスワードがユーザ識別情報と関連付けて一般端末で入力された場合に、これらのパスワードとユーザ識別情報とを受け取ってユーザデータとパスワードとの関連付けをデータベース上で設定する。これにより、ネットワークサービス提供装置からのサービスを受けるための会員であれば、一般端末を利用した内容に基づくユーザデータを、自己の個人端末から利用することができる。パスワードは、ネットワークサービス提供装置が適宜に発行し、かつそのパスワードはユーザの個人的使用に係る個人端末に通知される。さらに、パスワードは一般端末にて一回入力すれば、ユーザデータとアクセス識別情報とを対応付けるためにネットワークサービス提供装置及びユーザデータ管理装置にて用いられるか、又は利用する必要がなくなる。従って、先に述べたネットワークシステムと同様に、パスワードをユーザに低コストで提供でき、パスワードの発行や入力に関する安全性が高い。

【００２２】なお、このネットワークシステムにおいても、一般端末はゲームが実行される各種のコンピュータ機器を含む。さらには、ゲームセンターに設置されるアーケードゲーム機、インターネットカフェに設置されるパーソナルコンピュータ、スポーツクラブに設置されるトレーニングマシンのように、商業施設に設置され、不特定多数のユーザが利用可能な機器を一般端末とした場合に本発明は好適である。但し、一般端末の設置目的の営利、非営利は問わない。個人端末は、ネットワーク接続機能を有する各種のコンピュータ機器を含む。さらには、携帯電話、ＰＤＡ、携帯型ゲーム機のような個人的な使用を前提として構成されている情報機器が個人端末として使用される。家庭内に設置されるパーソナルコンピュータやビデオゲーム装置を個人端末として使用することもできる。但し、個人端末がユーザの所有に係るか否かは問わない。事実上ユーザが個人的に使用するコンピュータ機器であれば個人端末として使用可能である。

【００２３】パスワード管理手段は、所定のアルゴリズムによって一義的なパスワードを生成するものでもよいし、予め定められたパスワード群からいずれか一つのパスワードを抽出してアクセス識別情報と対応付けることにより、アクセス識別情報に対して一義的なパスワードを発行するものでもよい。パスワード通知手段は、文字列を利用してパスワードを通知するものでもよいし、音声信号によりパスワードを通知するものでもよい。

【００２４】個人端末上におけるユーザデータの利用は、ユーザデータの閲覧、ユーザデータの編集等の操作、ゲームに関するユーザデータに基づく個人端末上でのゲームのプレイなど、各種の態様を含む。

【００２５】本発明の他のネットワークシステムにおいて、前記個人端末は、個人端末からのアクセスに応答してその個人端末に固有の端末識別情報を特定し、その特定された端末識別情報を沿えてアクセス内容を通知する所定の通信処理システムを介して前記ネットワークサービス提供装置に接続される特定個人端末を含むことができる。例えば、インターネット接続機能を有する携帯電話はこうした通信処理システムを介して、ネットワーク上のサイトに接続される。このような特定個人端末を含む場合、前記ネットワークサービス提供装置（５）は、前記端末識別情報と前記ネットワークサービス提供装置からのサービス提供範囲で通用する会員毎の会員識別情報とを対応付けた会員情報テーブル（５ａ）を保有し、前記特定個人端末からアクセスがあった場合には、前記端末識別情報を前記アクセス識別情報として取得し、前記会員情報テーブルを参照して、その取得されたアクセス識別情報に対応する会員識別情報を特定する会員情報管理手段を具備し、前記パスワード管理手段は、前記会員識別情報に基づいて前記パスワードを発行することが望ましい。特定個人端末からのアクセスに伴って通知される端末識別情報は、個人端末からのユーザデータの利用を可能とする目的とは、本来的に異なる目的で使用されるため、こうした情報をユーザデータと対応付けるには種々の技術的あるいは商業的な制約が発生したり、何らかの法的規制が生じるおそれがある。これに対して端末識別情報を会員識別情報に変換し、その会員識別情報に基づいてパスワードを発行することとすれば、ネットワークシステム内における端末識別情報の利用を最小限に止めることができる。しかも、会員識別情報それ自体をユーザデータと直接対応付けるのではなく、パスワードを媒介として、いわば間接的に会員識別情報とユーザデータとを関連付けるので、一般端末の入力時等にパスワードが他人に盗まれたとしても、会員識別情報までが知られることはない。これにより、ネットワークサービス提供装置を利用した各種のサービスの安全性が、ユーザデータの利用という機能の追加によって損なわれるおそれもない。

【００２６】前記一般端末には、所定の記録媒体（２）に対する前記ユーザ識別情報の書き込みと、書き込まれたユーザ識別情報の読み込みとを行う読み書き手段と、前記記録媒体に有効なユーザ識別情報が記録されていない場合にユーザ識別情報の発行要求を出力する発行要求手段とが設けられ、前記ネットワークシステムには、前記発行要求手段からの要求に応じて新たなユーザ識別情報を発行して前記一般端末及び前記ユーザデータ管理装置に提供するユーザ識別情報管理装置（３）が設けられ、前記ユーザデータ管理装置（４）は、前記新たなユーザ識別情報を前記ユーザ識別情報管理装置から取得し、その取得されたユーザ識別情報を所定の初期ユーザデータと対応付けて前記データベース（４ａ）に記録し、前記一般端末の前記読み書き手段は、前記ユーザ識

別情報管理装置から前記新たなユーザ識別情報を取得した場合に、そのユーザ識別情報を前記記録媒体に記録する、ようにしてもよい。この場合、記録媒体がユーザに渡る前に記録媒体にユニークなＩＤを記録する必要がないので、記録媒体を安価に製造できる。また、ユーザが購入してから記録媒体に情報を書き込むため、ユーザに記録媒体を柔軟に運用させることができる。さらに、前記一般端末が複数の店舗のそれぞれに設置される一方で、前記ユーザデータ管理装置は前記複数の店舗の一般端末に共通して設置され、前記ユーザ識別情報管理装置は、各店舗の一般端末と前記ユーザデータ管理装置との間でかつ店舗毎に設けられてもよい。

【００２７】

【発明の実施の形態】図１は本発明の一実施形態に係るネットワークゲームシステムの構成を示す図である。このゲームシステムは、多数の店舗Ａとデータセンター Ｂとをインターネット Ｃで結んで構成されている。データセンターＢは、各店舗Ａで発生するゲームデータを一括管理している。このため、ユーザは店舗Ａでプレイした自己のゲームデータを、他の店舗Ａにおいても利用することができる。また、データセンターＢは、携帯電話６からアクセス可能な会員制のウェブサイトを運営している。データセンターＢは、ゲームソフトのダウンロードサービスやイベント情報の提供など、様々なサービスを会員に提供している。そのサービスの一つとして、店舗Ａでプレイされるゲームに関する所定のサービスも提供する。例えば、ウェブサイトの会員となっているユーザは、携帯電話６などの個人端末からネットワークを介してデータセンターＢにアクセスすることで、店舗Ａでプレイした自己のゲームデータを利用することができる。

【００２８】各店舗Ａには複数のゲーム機（一般端末に相当）１…１が設置されている。ユーザは磁気テープ、ＩＣ等の記録媒体を含むエントリーカード２をいずれかのゲーム機１に挿入してゲームを開始する。ゲーム機１は、エントリーカード２に記録されているユーザ識別情報としてのＩＤを読み取り、そのＩＤに対応するプレイヤーデータ（ユーザ毎のゲームデータに相当）に基づいたゲームをユーザに提供する。プレイヤーデータは、ＩＤに関する情報とユーザのゲーム履歴に基づく情報を含んで生成される各ユーザ毎に異なるデータである。プレイヤーデータの詳細は後述する。各ゲーム機１は、各店舗に１台設置された店舗サーバー（ユーザ識別情報管理装置）３とＬＡＮなどのネットワークを介して接続されている。店舗サーバー３は、自己の店舗で利用されたプレイヤーデータを店舗プレイヤーテーブル３ａに記録している。店舗サーバー３は、インターネットなどのネットワークを介してデータセンターに設置されたセンターサーバー（ゲームデータ管理装置）４に接続されている。センターサーバー４は、全ての店舗で利用されたプレイヤーデータをセンタープレイヤーテーブル４ａに記録している。センターサーバー４はＬＡＮ等のネットワークを介して、データセンターに設置された携帯サイトサーバー５に接続されている。携帯サイトサーバー（ネットワークサービス提供装置）５は、携帯電話６からアクセス可能な会員制のウェブサイトを運営している。携帯サイトサーバー５は会員に関する情報を会員番号テーブル５ａに記録している。

【００２９】図２（ａ）は会員番号テーブル５ａの内容を示している。会員番号テーブル５ａには、携帯サイトサーバーへアクセスした携帯電話６の所有者を特定するための携帯ＩＤ（アクセス識別情報、機器識別情報）と、携帯サイトサーバーが運営するウェブサイトの会員番号（会員識別情報）とが対応付けて記録される。携帯ＩＤはユーザが携帯電話６から携帯サイトサーバー５にアクセスした場合、電話会社によって携帯サイトサーバー５に通知されるものであり、携帯電話毎に固有の値である。電話会社は、携帯電話６からの発信があると、その携帯電話６の携帯ＩＤを特定し、携帯電話６からのアクセス内容に対応した情報にその携帯ＩＤを添えて携帯サイトサーバー５に通知する通信処理ネットワーク（不図示）を運営している。

【００３０】図２（ｂ）は店舗プレイヤーテーブル３ａ、センタープレイヤーテーブル４ａの内容を示している。それぞれのテーブルに記録されるプレイヤーデータは、ＩＤに関する情報と、プレイヤーデータが更新された日付（日時）に関する情報と、会員番号から一義的に生成されるパスワードに関する情報と、キャラクタの状態に関する情報とを含んでいる。キャラクタの状態を示す情報は、キャラクタの名前、レベル、所有するアイテム等に関する情報を含んでいる。なお、パスワードが無効である（まだ登録されていない）場合には、パスワードに関する情報はＮＵＬＬとなっている。

【００３１】図３は、携帯電話６及び携帯サイトサーバー５がそれぞれ実行するパスワード発行処理の手順を示すフローチャートである。この処理は携帯電話６が携帯サイトサーバー５にアクセスしてパスワードの発行を要求したときに開始される。ユーザが携帯電話６に所定の操作を行うと、携帯電話６は携帯サイトサーバー５にパスワード発行要求を送信し（ステップＳ６０１）、その後、ステップＳ６０２にてパスワードの送信を待つ。パスワード発行要求を受信した携帯サイトサーバー５は、パスワード発行要求を送信した携帯電話６の携帯ＩＤから、会員番号を特定する（ステップＳ５０１）。なお、携帯ＩＤは携帯電話６が携帯サイトサーバー５にアクセスした際に、電話会社から携帯サイトサーバー５に通知されている。次に、その会員番号を暗号化することによって、会員番号に対して一義的に定まるパスワードを生成し（ステップＳ５０２）、携帯電話６に送信する（ステップＳ５０３）。携帯電話６は、パスワードを受信すると、例えば図４の画面１０のように、画面上にそのパ

スワードを表示する（ステップＳ６０３）。これにより、ユーザは自己の携帯に対応するパスワードを取得する。

【００３２】図５は、ゲーム機１が実行するゲーム開始から終了までの処理の手順を示すフローチャートである。この処理は、ユーザによってゲーム機１にエントリーカード２が挿入されるとともに、ゲーム開始のための所定の操作が行われることにより開始される。まず、ゲーム機１はエントリーカード２にＩＤが記録されているか否かを判定する（ステップＳ１０１）。ＩＤが記録されていないと判定した場合は、ＩＤ発行要求を店舗サーバー３へ送信する（ステップＳ１０２）。すなわち、初めてのプレイと判断し、初回登録処理を店舗サーバー３に要求する。ＩＤ発行要求を受信した店舗サーバー３の処理については後述する。ゲーム機１はステップＳ１０３にて、店舗サーバー３からユニークなＩＤを含む初期状態のプレイヤーデータが送信されるのを待つ。プレイヤーデータを受信した場合は、そのプレイヤーデータに含まれるＩＤをエントリーカード２に書き込む（ステップＳ１０４）。次に、そのプレイヤーデータをユーザにカスタマイズさせるための処理を行い（ステップＳ１０５）、カスタマイズされたプレイヤーデータを店舗サーバー３へ送信する（ステップＳ１０６）。

【００３３】ステップＳ１０１にて、エントリーカード２にＩＤが記録されていると判定した場合は、そのＩＤを店舗サーバー３に送信する（ステップＳ１０７）。すなわち、２回目以降のプレイと判断し、そのＩＤに対応するプレイヤーデータの送信を要求する。ＩＤを受信した店舗サーバー３の処理については後述する。ゲーム機１はステップＳ１０８にて、店舗サーバー３から送信したＩＤに対応するプレイヤーデータが送信されるのを待つ。受信した場合はステップＳ１０９に進む。

【００３４】ステップＳ１０９では、プレイヤーデータに基づき、ユーザにゲームをプレイさせるための処理を実行する。ゲームオーバーとなると、ゲームの進行状況に応じて変更されたプレイヤーデータを店舗サーバー３に送信し（ステップＳ１１０）、処理を終了する。

【００３５】図６は、店舗サーバー３及びセンターサーバー４が実行する初回登録処理の手順を示すフローチャートである。この処理は、ゲーム機１から送信されたＩＤ発行要求（図５のステップＳ１０２参照）を店舗サーバー３が受信したときに開始される。店舗サーバー３は、ゲーム機１からＩＤ発行要求を受信すると、ユニークなＩＤを発行するとともに、そのＩＤを含む初期状態のプレイヤーデータを作成する（ステップＳ３０１）。次にゲーム機１にそのプレイヤーデータを送信する（ステップＳ３０２）。送信したデータは図５のステップＳ１０３にて待機していたゲーム機１に受信される。ステップＳ１０６（図５）にてゲーム機１がプレイヤーデータを送信すると、図６のステップＳ３０３にてそのプレイヤーデータの受信まで待機していた店舗サーバー３は、そのプレイヤーデータに日付（日時）をつけて店舗プレイヤーテーブル３ａに記録する（ステップＳ３０４）。なお、パスワードに関する情報を記録すべき部分は無効である印としてＮＵＬＬとなっている（図２（ｂ）参照）。次に、そのプレイヤーデータをセンターサーバー４に送信する（ステップＳ３０５）。センターサーバー４は、その受信したプレイヤーデータをセンタープレイヤーテーブル４ａに記録し（ステップＳ４０１）、その記録した日時に関する情報を店舗サーバー３に送信する（ステップＳ４０２）。ステップＳ３０６にて日時に関する情報の受信まで待機していた店舗サーバー３は、受信した日時に基づいて、ステップＳ３０４にて記録したプレイヤーデータの日時を修正し（ステップＳ３０７）、初回登録処理を終了する。

【００３６】図７は、店舗サーバー３及びセンターサーバー４が実行するデータ送信処理の手順を示すフローチャートである。この処理は、ゲーム機１から送信されたＩＤ（図５のステップＳ１０７参照）を店舗サーバー３が受信したときに開始される。ゲーム機１からＩＤを受信した店舗サーバー３は、そのＩＤに対応するプレイヤーデータが店舗プレイヤーテーブル３ａに記録されているか否か判定する（ステップＳ３１１）。記録されていると判定した場合は、そのプレイヤーデータをセンターサーバー４に送信し（ステップＳ３１２）、記録されていないと判定した場合は、そのＩＤをセンターサーバー４に送信する（ステップＳ３１３）。センターサーバー４は、プレイヤーデータを受信したのか、ＩＤを受信したのかを判定する（ステップＳ４１１）。プレイヤーデータを受信したと判定した場合は、受信したプレイヤーデータに含まれるＩＤに対応するプレイヤーデータを、センタープレイヤーテーブル４ａから検索し、受信したプレイヤーデータの日付と、センタープレイヤーテーブル４ａに記録されているプレイヤーデータの日付とを比較し、何れが新しいデータかを判定する（ステップＳ４１２）。受信したプレイヤーデータの方が新しいと判定した場合は、センタープレイヤーテーブル４ａのプレイヤーデータを更新し（ステップＳ４１３）、店舗サーバー３に“ＯＫ”のサインを送信する（ステップＳ４１４）。ステップＳ４１１にてＩＤを受信したと判定した場合は、そのＩＤに対応するプレイヤーデータをセンタープレイヤーテーブル４ａから検索して店舗サーバー３に送信する（ステップＳ４１５）。また、ステップＳ４１２にて、センタープレイヤーテーブル４ａに記録されているプレイヤーデータの方が受信したプレイヤーデータよりも新しいと判定した場合にも、センタープレイヤーテーブル４ａに記録されているプレイヤーデータを送信する（ステップＳ４１５）。ステップＳ３１４にてセンターサーバー４からのデータ照会の結果を待っていた店舗サーバー３は、ステップＳ３１５にて、プレイヤー

データを受信したのか、“ＯＫ”のサインを受信したのかを判定する。プレイヤーデータを受信したと判定した場合は、受信したプレイヤーデータにより店舗プレイヤーテーブル３ａを更新する（ステップＳ３１６）。その後、そのプレイヤーデータをゲーム機１へ送信する（ステップＳ３１７）。ステップＳ３１５にて、“ＯＫ”のサインを受信したと判定した場合は、ステップＳ３１６をスキップし、プレイヤーデータをゲーム機１に送信する（ステップＳ３１７）。ステップＳ３１７にて送信されたプレイヤーデータは、図５のステップＳ１０８にて待機していたゲーム機１に受信される。

【００３７】図８は、ゲーム機１が実行するパスワード登録処理の手順を示すフローチャートである。この処理は、ユーザによってゲーム機１にエントリーカード２が挿入されるとともに、携帯サイトサーバー６が運営するウェブサイトの会員番号とエントリーカード２に記録されたＩＤとを対応付けるための所定の操作が行われたときに開始される。まず、ゲーム機１はエントリーカード２に記録されたＩＤに関する情報を読み取り、ＩＤが記録されているか否かを判定する（ステップＳ１２１）。ＩＤが記録されていなければ処理を終了する。ＩＤが記録されている場合は、ユーザにパスワードを入力させるための処理を実行し、パスワードが入力されたか否かを判定する（ステップＳ１２２）。パスワード入力がキャンセルされた場合は処理を終了する。パスワードが入力された場合は、入力されたパスワードが有効か否か判定する（ステップＳ１２３）。つまり、ユーザがでたらめなパスワードを入力していないか否かを判定する。従って、図３のステップＳ５０２においては、パスワードにエラーチェックのための文字を含ませる等、パスワードからそのパスワードが有効なものであるか否かを検出できるように、パスワードを生成しておく。図８のステップＳ１２３にて、パスワードが有効でないと判定した場合は処理を終了する。有効と判定した場合は、ＩＤとパスワードとを店舗サーバー３に送信する（ステップＳ１２４）。ＩＤとパスワードとを受信したときに店舗サーバー３が実行する処理については後述する。ゲーム機１は店舗サーバー３からパスワードが登録できたか否かの結果を待ち（ステップＳ１２５）、登録結果を受信した場合には、その結果をユーザに表示するなどした後、処理を終了する。

【００３８】図９は、店舗サーバー３及びセンターサーバー４が実行するパスワード登録処理の手順を示すフローチャートである。この処理は、ゲーム機１から送信されたＩＤとパスワードと（図８のステップＳ１２４参照）を店舗サーバー３が受信したときに開始される。店舗サーバー３は、受信したＩＤとパスワードとをセンターサーバー４に送信する（ステップＳ３２１）。センターサーバー４は、受信したＩＤに対応するプレイヤーデータをセンターサーバー４ａから検索する（ステップＳ４２１）。次に、該当するプレイヤーデータのパスワードに関する情報がＮＵＬＬであるか否かを判定する（ステップＳ４２２）。ＮＵＬＬである場合には、受信したパスワードをそのプレイヤーデータのパスワードに関する情報として記録し（ステップＳ４２３）、パスワード登録成功のサインを店舗サーバー３に送信する（ステップＳ４２４）。ステップＳ４２２にて、パスワードに関する情報がＮＵＬＬでないと判定した場合は、ステップＳ４２３をスキップし、既に登録済みである旨のサインを店舗サーバー３に送信する（ステップＳ４２４）。ステップＳ３２２にて、登録結果を待っていた店舗サーバー３は、登録結果が成功のサインであると判定した場合、店舗プレイヤーテーブル３ａの該当するプレイヤーデータを検索し、そのパスワードを記録する（ステップＳ３２４）。次にゲーム機１へパスワード登録成功のサインをゲーム機１に送信する（ステップＳ３２５）。ステップＳ３２３にて登録結果が既に登録済みである旨のサインと判定した場合は、ステップＳ３２４をスキップし、既に登録済みである旨のサインをゲーム機１に送信する（ステップＳ３２５）。送信した登録結果は、図８のステップＳ１２５にて待機していたゲーム機１に受信される。

【００３９】図１０は、センターサーバー４及び携帯サイトサーバー５が実行するデータ送信処理の手順を示すフローチャートである。この処理は、ユーザが携帯電話６から携帯サイトサーバー５に対して、所定の操作によって自己のプレイヤーデータの送信を要求したときに開始される。ユーザからプレイヤーデータの送信要求があったとき、携帯サイトサーバー５は、携帯ＩＤに対応する会員番号を特定する（ステップＳ５３１）。次に、図３のステップ５０２と同一の暗号化方法により、その会員番号に一義的に定まるパスワードを作成し（ステップＳ５３２）、センターサーバー４に送信する（ステップＳ５３３）。パスワードを受信したセンターサーバー４は、そのパスワードを含むプレイヤーデータをセンタープレイヤーテーブル４ａから検索する（ステップＳ４３１）。次に該当するプレイヤーデータを携帯サイトサーバー５へ送信する（ステップＳ４３２）。ステップＳ５３４にてプレイヤーデータの送信を待っていた携帯サイトサーバー５は、受信したプレイヤーデータを送信を要求したユーザの携帯電話６へ送信する（ステップＳ５３５）。

【００４０】なお、センターサーバー４が、パスワードに関する情報が有効か無効（ＮＵＬＬ）かで携帯サイト入会特典の有無を判定してもよい。例えば、登録してある携帯電話６のユーザにメールを発行するなどの特典により、携帯サイトへの入会を促すことができる。また、ステップＳ４２３、Ｓ３２４において、パスワードの代わりに、パスワードを更に暗号化した情報等のパスワードに基づいて一義的に定まる情報を用い、それ以降はパ

スワードを一切使用しないようにして更にセキュリティを高めてもよい。

【００４１】図１１～図１８は、図３～図９までの処理を図解するものである。以下、図１１に示す状態から新規のユーザがゲームを開始する場合を例に挙げて本発明のネットワークゲームシステムの処理をさらに説明する。

【００４２】図１１は、店舗プレイヤーテーブル３ａ及び店舗プレイヤーテーブル４ａに、ＩＤが１～３のプレイヤーデータが記録されている状況を示している。

【００４３】図１２は、携帯サイトサーバー５が新規なユーザ５０にパスワードを発行するときの状況を示している（図３、図４参照）。ユーザ５０は携帯サイトサーバー５が運営しているウェブサイトの会員であり、携帯電話６から携帯サイトサーバー５に対しパスワード発行を要求する。要求を受信した携帯サイトサーバー５はパスワードを発行し、携帯電話６に表示させる。

【００４４】図１３及び図１４は、ユーザ５０がゲーム機１にて初めてプレイするときのゲーム機１や各サーバーの状況を示している（図５、図６参照）。図１３では、ユーザはコインを投入し、未使用の（まだＩＤが記録されていない）エントリーカード２をゲーム機１に挿入する。ゲーム機１はエントリカード２にまだＩＤが記録されていないことを検出し、店舗サーバー３にＩＤ発行要求を送信する。店舗サーバー３はＩＤを発行するとともに、そのＩＤを含むプレイヤーデータを作成し、ゲーム機１に送信する。図１４では、ユーザがカスタマイズしたプレイヤーデータがゲーム機１から店舗サーバー３に送信される。店舗サーバー３はそのデータに日付をつけて店舗プレイヤーサーバー３ａに記録する。同図では、ＩＤ＝４のプレイヤーデータがユーザ５０のプレイヤーデータとして新たに追加される。なお、このときパスワードの欄は無効である印としてＮＵＬＬとなっている。店舗サーバー３はこのプレイヤーデータをセンターサーバー４に送信する。センターサーバー４は受信したプレイヤーデータをセンタープレイヤーテーブル４ａに記録する。次にセンターサーバー４は日付を店舗サーバー３に送信する。店舗サーバー３は店舗プレイヤーテーブル３ａに記録されているＩＤ＝４のプレイヤーデータの日付を修正する。

【００４５】図１５及び図１６は、ユーザ５０がパスワードを登録するときにゲーム機１及び各サーバの状況を示している（図８、図９参照）。図１５では、ユーザ５０はゲーム機１にエントリーカード２を挿入するとともに、パスワードを入力する。パスワード及びエントリーカード２から読み取られたＩＤは、ゲーム機１から店舗サーバー３を経由してセンターサーバー４に送信される。センターサーバー４は、このＩＤが含まれるプレイヤーデータを検索する。該当するプレイヤーデータのパスワードの欄がＮＵＬＬであれば、そこにパスワードを記録する（同図ではＩＤ＝４のプレイヤーデータ）。図１６では、センターサーバー４はパスワードの登録が成功か失敗かを店舗サーバー３へ通知する。成功ならば、店舗サーバー３は店舗プレイヤーテーブル３ａのＩＤ＝４のプレイヤーデータにパスワードを記録する。店舗プレイヤーサーバー３はゲーム機１にパスワードの登録が成功か失敗かをゲーム機１に通知する。

【００４６】図１７及び図１８は、ユーザ５０が２回目以降のプレイをするときにゲーム機１及び各サーバーの状況を示している（図５、図７参照）。図１７では、ユーザ５０はゲーム機１にコインを入れ、エントリーカードを挿入する。既にパスワード登録が終わっていれば、パスワードを入力する必要はない。ゲーム機１はエントリーカード２からＩＤを読み取り（同図ではＩＤ＝４）、そのＩＤを含むプレイヤーデータを店舗サーバー３に要求する。店舗サーバー３は、店舗プレイヤーテーブル３ａに該当するプレイヤーデータがあればそのプレイヤーデータを、なければＩＤをセンターサーバー４に送信し、プレイヤーデータを要求する。センターサーバー４は、該当するプレイヤーデータ（ＩＤ＝４）をセンタープレイヤーテーブル４ａから読み出す。図１８では、センターサーバー４は、図１７にて店舗サーバー３から出された要求に応じてプレイヤーデータ等を送信する。すなわち、店舗サーバー３からプレイヤーデータを受信していた場合は、受信したプレイヤーデータの日付とセンターサーバー４ａの該当するプレイヤーデータの日付とを比較し、センターサーバー４ａの方が新しければそのプレイヤーデータを、受信したプレイヤーデータの方が新しければ“ＯＫ”のサインを送信する。店舗サーバー３からＩＤを受信していた場合は、センターサーバー４ａの該当するプレイヤーデータを送信する。なお、センターサーバー４ａに該当するプレイヤーデータがない等の何らかのエラーが発生した場合は“ＢＡＤ”のサインを送信する。店舗サーバー３は“ＯＫ”を受信した場合は、店舗プレイヤーテーブル３ａのプレイヤーデータをゲーム機１に送信する。プレイヤーデータを受信した場合は、そのプレイヤーデータを店舗プレイヤーテーブル３ａに記録（更新）するとともに、ゲーム機１に送信する。

【００４７】以上のように、本実施形態によれば、ステップＳ４２３及びステップＳ３２４（図９）の処理により、ゲーム機１にてプレイヤーデータを用いてゲームをプレイするためのＩＤと、携帯サイトサーバー５が運営するウェブサイトのサービスを受けるための会員番号とが、パスワードによって対応付けられる。パスワードは、ユーザが携帯電話６から発行を要求したときに、携帯サイトサーバー５により発行されるため（図３のステップＳ５０２）、エントリーカード２に印刷して製造販売する必要がない。また、パスワードは、携帯電話６の画面上に表示されるため（図３のステップＳ６０３）、

ゲーム機１に表示する場合に比較して他のユーザに盗まれるおそれがない。さらに、このパスワードはステップＳ１２２（図８）にてゲーム機１に一回入力すれば、ＩＤと会員番号とを対応付けるためにゲームシステム内部で用いられるだけであり、それ以上ゲーム機１及び携帯電話６から入力する必要がない。従って、セキュリティの高いユーザ認証システムを安価に実現できるネットワークゲームシステムを提供できる。

【００４８】なお、本発明は以上の実施形態に限定されず、種々の形態にて実施してよい。例えば、店舗サーバー３とセンターサーバー４、センターサーバー４と携帯サイトサーバー５は統合してもよいし、これら３つを統合してもよい。逆に、各サーバーをさらに分散して、各サーバーの負担を軽減してもよい。ＩＤの発行や初期状態のプレイヤーデータの生成をゲーム機１が実行してもよい。店舗サーバー３にゲーム進行状況の中継モニターとしての機能を含めてもよいし、センターサーバー４にゲーム進行状況を一元管理する機能やゲーム進行状況を各店舗サーバー３に送信する機能を含めてもよい。受信したパスワードが存在するか否かを携帯サイトサーバー５に確認する機能をセンターサーバー４に含めてもよい。エントリーカード２は磁気、ＩＣを利用したものに限られず、ＩＤを記録できるものであればよい。ＩＤはエントリーカードに最初から記録されていてもよい。パスワードは会員番号に基づくものに限られず、個人端末にてサービスを受けるユーザを特定するものであればよく、携帯ＩＤから直接生成してもよい。また、パスワードはユーザを特定する情報を暗号化したものでなくとも、他のユーザによってパスワードからユーザを特定する情報を認知されなければよい。例えば、ランダムに発生させた文字列をパスワードとして用い、そのパスワードを会員番号と対応付けて記録しておくことにより、会員番号からパスワードを参照できるようにしてもよい。

【００４９】本発明のネットワークシステムは、ゲーム機又はゲーム端末を一般端末として使用するものに限定されず、種々の用途に適用できる。例えば、スポーツクラブのトレーニングマシンを一般端末として設定した場合、そのトレーニングマシンの利用内容に基づくユーザデータ（例えば運動時間、消費エネルギー）をデータベースに記録し、そのユーザデータを携帯電話等の個人端末から利用可能とする場合にも本発明は適用できる。この場合、個人端末からのユーザデータの利用は、例えば個人端末上で運動時間等を参照して食事内容の選択の参考としたり、あるいは実際に摂取した食事内容を個人端末から送信してデータベースを更新し、それにより、ユーザの個人の日常生活をスポーツクラブにおけるトレーニングメニューの決定に反映させるような使用形態が可能である。

【００５０】

【発明の効果】以上に説明したように、本発明によれば、パスワードを媒介としてアクセス識別情報とユーザデータとが関連付けられ、そのパスワードはシステムが適宜に発行するためにユーザに低コストで提供でき、パスワードがユーザの個人使用に係る個人端末に表示されるために他のユーザにパスワードを盗まれる可能性が低く、一般端末にパスワードが一旦入力された後は、アクセス識別情報とユーザデータとを対応付ける媒介としてパスワードがシステムの内部で用いられるか、あるいは全く利用されないようになり、一般端末や個人端末から再びパスワードを入力する必要はない。従って、一般端末の利用内容に基づいて生成されてユーザ識別情報と対応付けて記録されるユーザデータを、一般端末とは異なる携帯電話等の個人端末から利用可能とするために必要な情報（パスワード）の発行や入力に際しての安全性が高く、かつそのような情報を低コストでユーザに提供することが可能なネットワークシステムを実現することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワークゲームシステムの構成を示す図。

【図２】図１のネットワークゲームシステムの記憶手段に記録されるデータの内容を示す図。

【図３】携帯電話と、携帯サイトサーバーとが実行するパスワード発行処理の手順を示すフローチャート。

【図４】図３の処理における携帯電話の画面の例を示す図。

【図５】ゲーム機が実行するゲーム開始から終了までの処理の手順を示すフローチャート。

【図６】店舗サーバー及びセンターサーバーが実行する初回登録処理の手順を示すフローチャート。

【図７】ゲーム機からデータ送信の要求があったときに、店舗サーバー及びセンターサーバーが実行するデータ送信処理の手順を示すフローチャート。

【図８】ゲーム機が実行するパスワード登録処理の手順を示すフローチャート。

【図９】店舗サーバー３及びセンターサーバー４が実行するパスワード登録処理の手順を示すフローチャート。

【図１０】携帯電話からデータの送信の要求があったときに、センターサーバー及び携帯サイトサーバーが実行するデータ送信処理の手順を示すフローチャート。

【図１１】ゲームシステムの１状況例を示す図。

【図１２】パスワードを発行するときの状況例を示す図。

【図１３】ユーザが初めてプレイするときの状況例を示す図。

【図１４】ユーザが初めてプレイするときの状況例を示す図。

【図１５】ユーザがパスワードを登録するときの状況例を示す図。

【図１６】ユーザがパスワードを登録するときの状況例

を示す図。

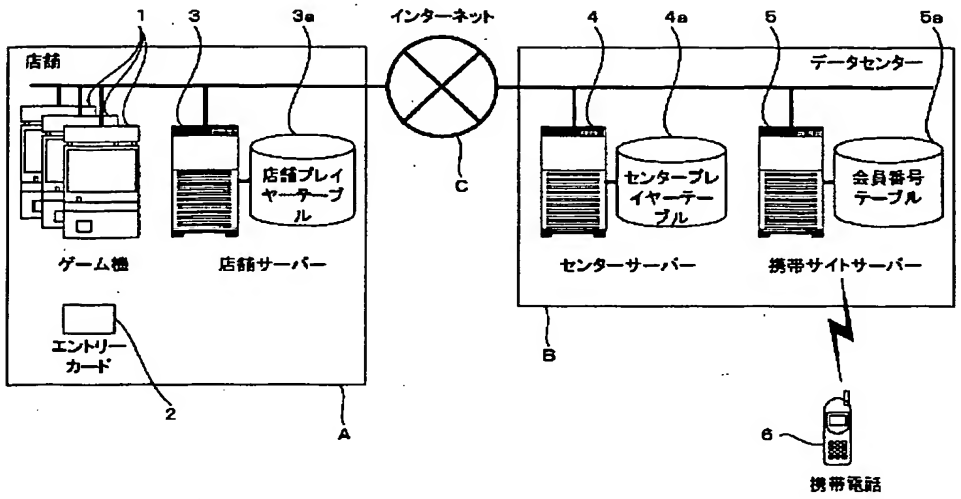
【図１７】ユーザが２回目以降のプレイをするときの状況例を示す図。

【図１８】ユーザが２回目以降のプレイをするときの状況例を示す図。

【符号の説明】

1　ゲーム機
2　エントリーカード
3　店舗サーバー
3ａ　店舗プレイヤーテーブル
4　センターサーバー
4ａ　センタープレイヤーテーブル
5　携帯サイトサーバー
5ａ　会員番号テーブル
6　携帯電話

【図１】



【図２】

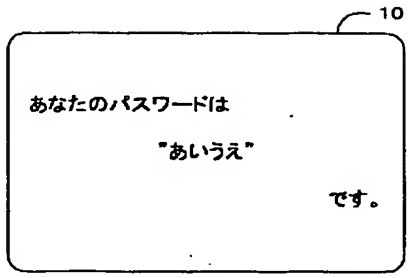
(a)

携帯ID	会員番号
645	311
356	312
238	313

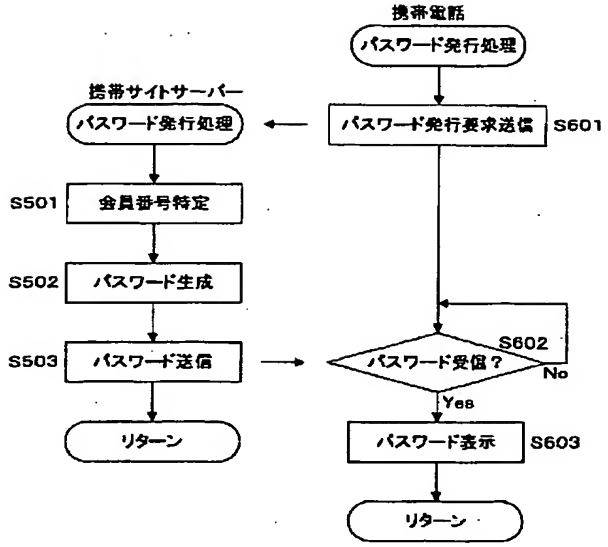
(b)

ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大竜巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…

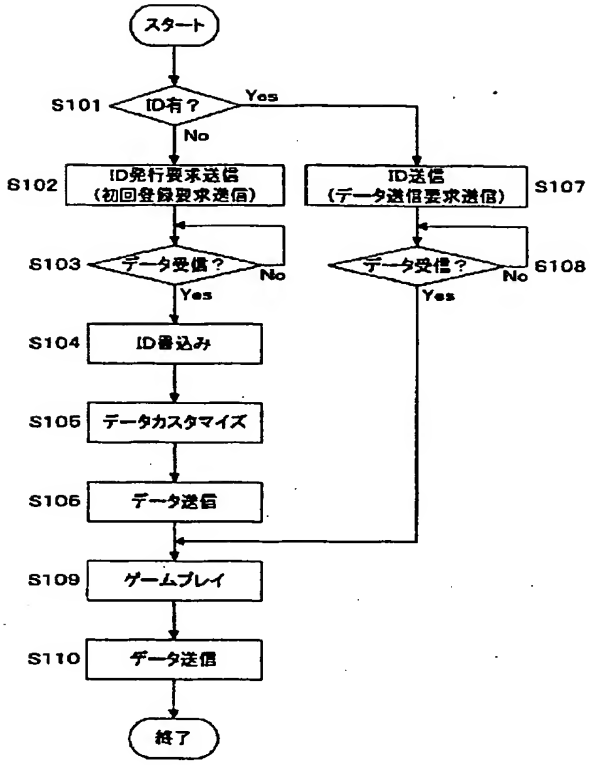
【図４】



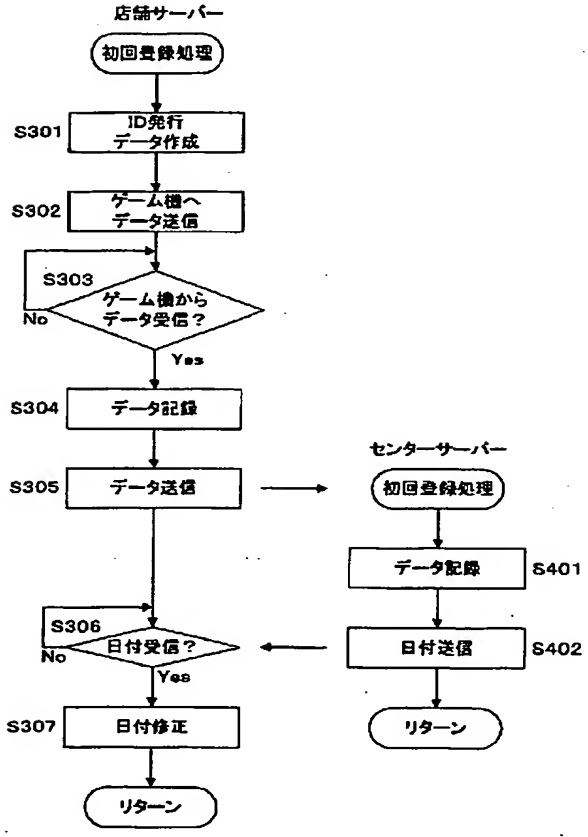
【図３】


携帯電話
パスワード発行処理
携帯サイトサーバー
パスワード発行処理
パスワード発行要求送信
S601
S501
会員番号特定
S502
パスワード生成
S503
パスワード送信
S602
パスワード受信？
No
Yes
リターン
パスワード表示
S603
リターン

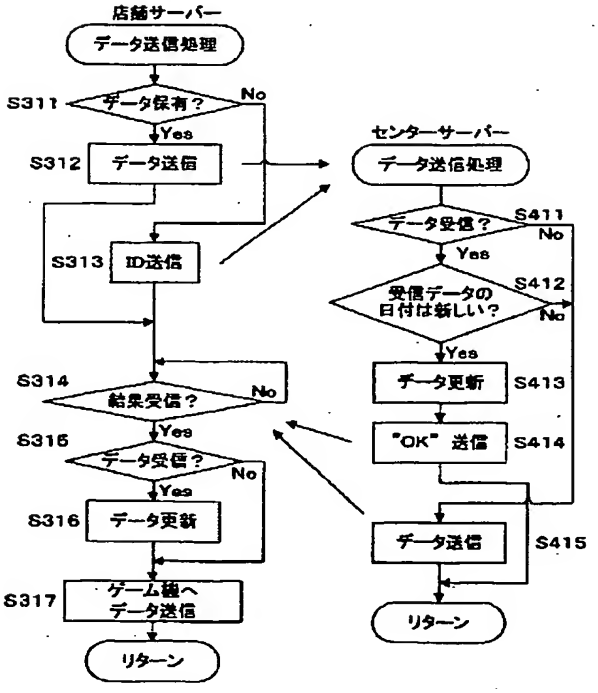
【図５】


スタート
S101
ID有？
Yes
No
S102
ID発行要求送信
（初回登録要求送信）
ID送信
（データ送信要求送信）
S107
S103
データ受信？
No
Yes
データ受信？
No
S108
Yes
S104
ID書込み
S105
データカスタマイズ
S106
データ送信
S109
ゲームプレイ
S110
データ送信
終了

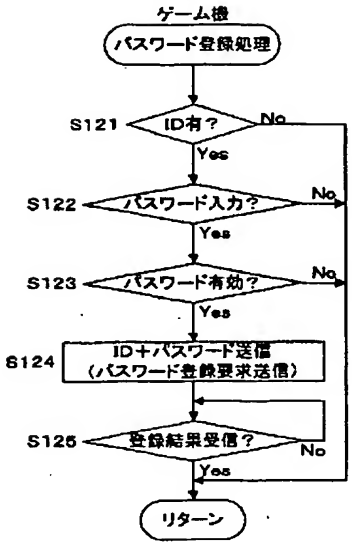
【図６】


店舗サーバー
初回登録処理
S301
ID発行
データ作成
S302
ゲーム機へ
データ送信
S303
ゲーム機から
データ受信？
No
Yes
S304
データ記録
S305
データ送信
センターサーバー
初回登録処理
データ記録
S401
S306
日付受信？
No
Yes
日付送信
S402
S307
日付修正
リターン
リターン

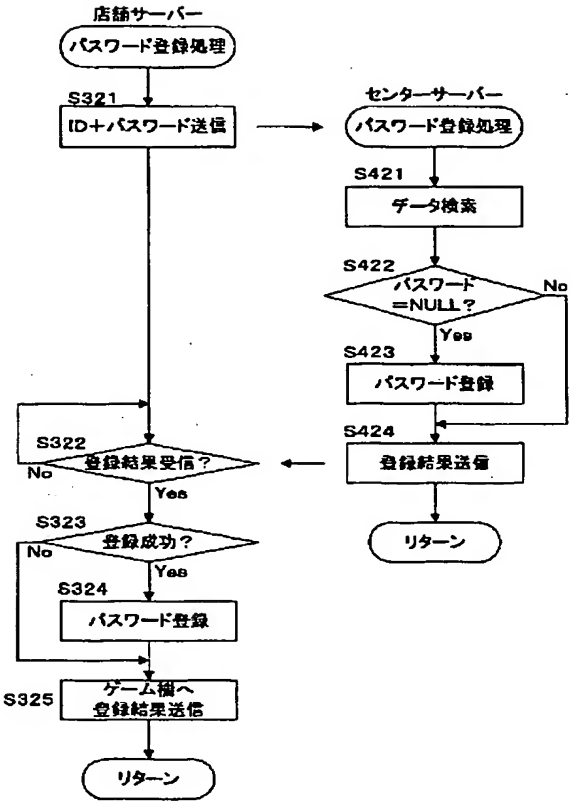
【図７】


店舗サーバー
データ送信処理
S311
データ保有？
No
Yes
S312
データ送信
センターサーバー
データ送信処理
S411
データ受信？
No
Yes
S313
ID送信
S412
受信データの
日付は新しい？
No
Yes
S314
結果受信？
No
Yes
S413
データ更新
S315
データ受信？
No
Yes
S414
"OK" 送信
S316
データ更新
S415
データ送信
S317
ゲーム機へ
データ送信
リターン
リターン

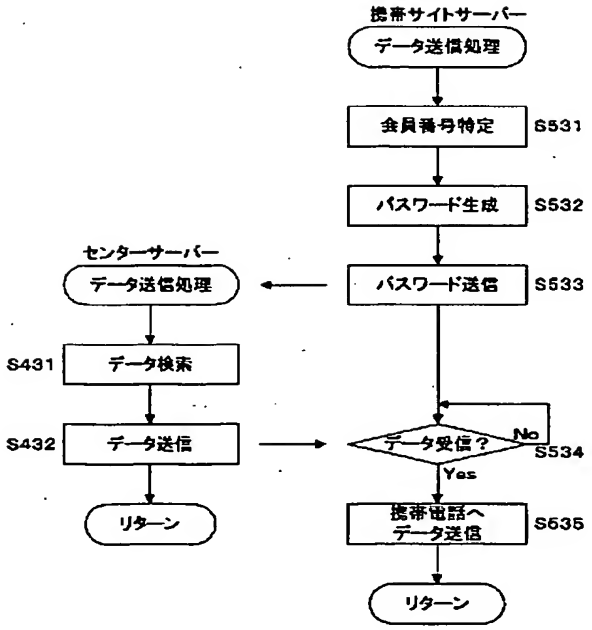
【図８】


ゲーム機
パスワード登録処理
S121
ID有？
No
Yes
S122
パスワード入力？
No
Yes
S123
パスワード有効？
No
Yes
S124
ID＋パスワード送信
（パスワード登録要求送信）
S125
登録結果受信？
No
Yes
リターン

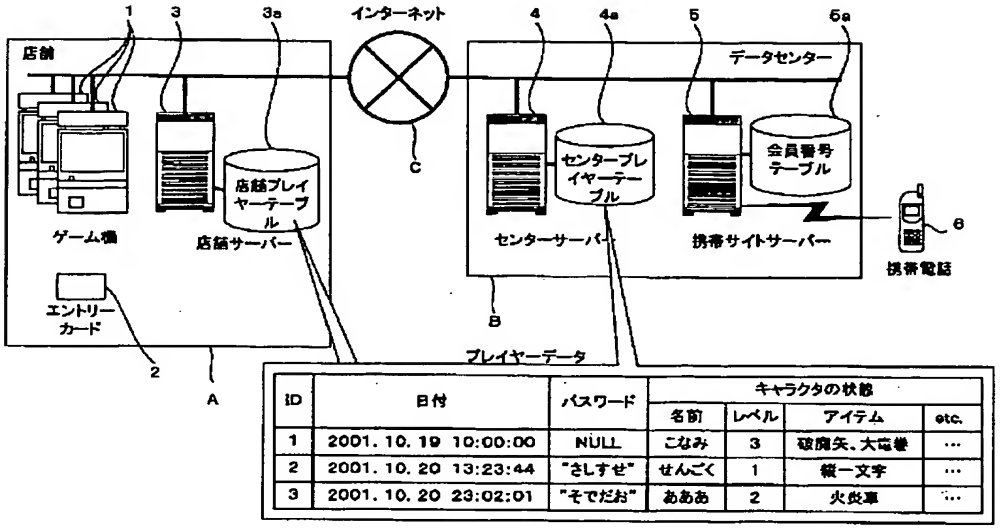
【図９】


店舗サーバー
パスワード登録処理
S321
ID＋パスワード送信
センターサーバー
パスワード登録処理
S421
データ検索
S422
パスワード
＝NULL？
No
Yes
S423
パスワード登録
S424
登録結果送信
リターン
S322
登録結果受信？
No
Yes
S323
登録成功？
No
Yes
S324
パスワード登録
S325
ゲーム機へ
登録結果送信
リターン

【図１０】

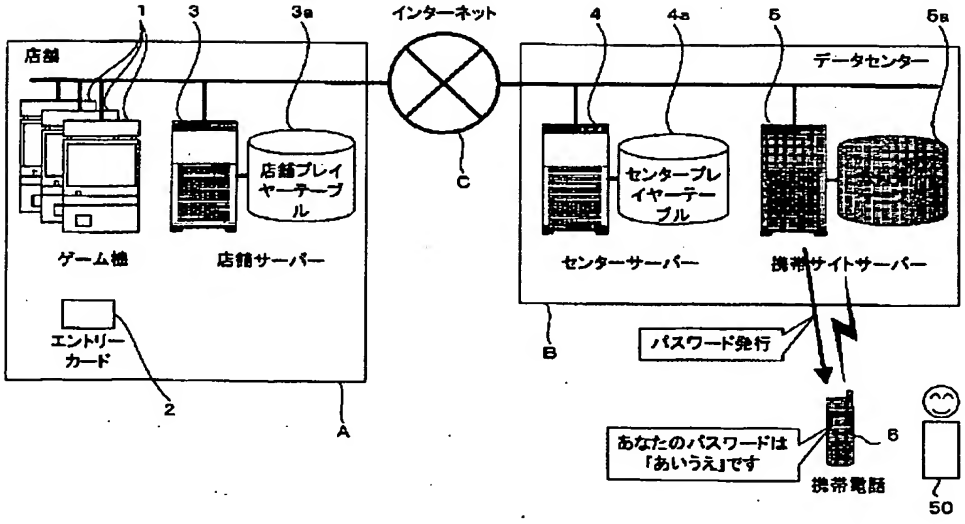

携帯サイトサーバー
データ送信処理
会員番号特定
S531
パスワード生成
S532
パスワード送信
S533
センターサーバー
データ送信処理
S431
データ検索
S432
データ送信
リターン
データ受信？
No
S534
Yes
携帯電話へ
データ送信
S535
リターン

【図１１】

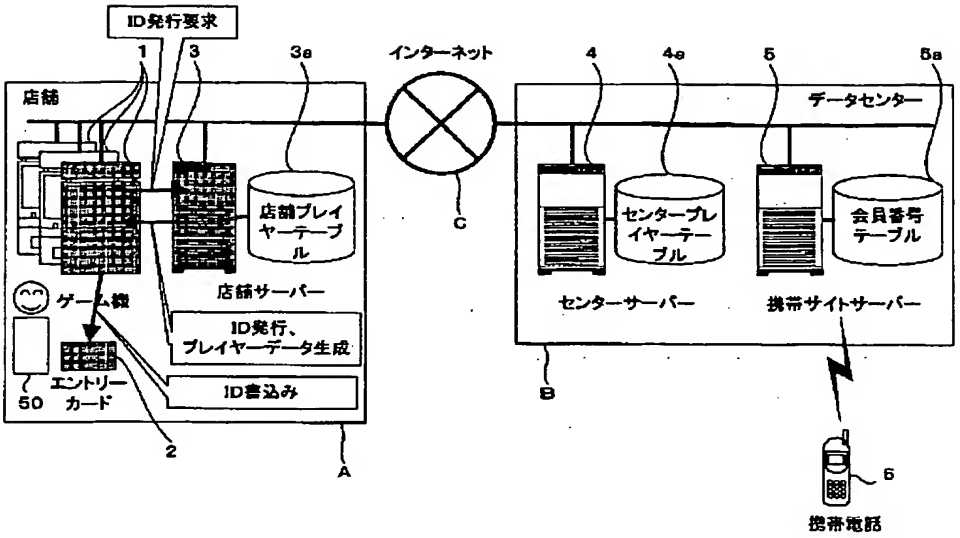


ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大吸巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	あああ	2	火炎車	…

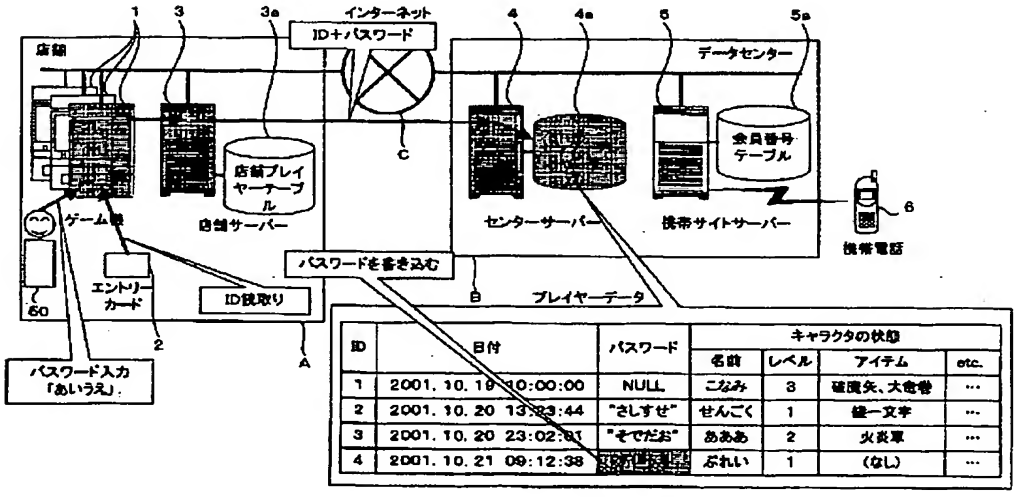
【図１２】



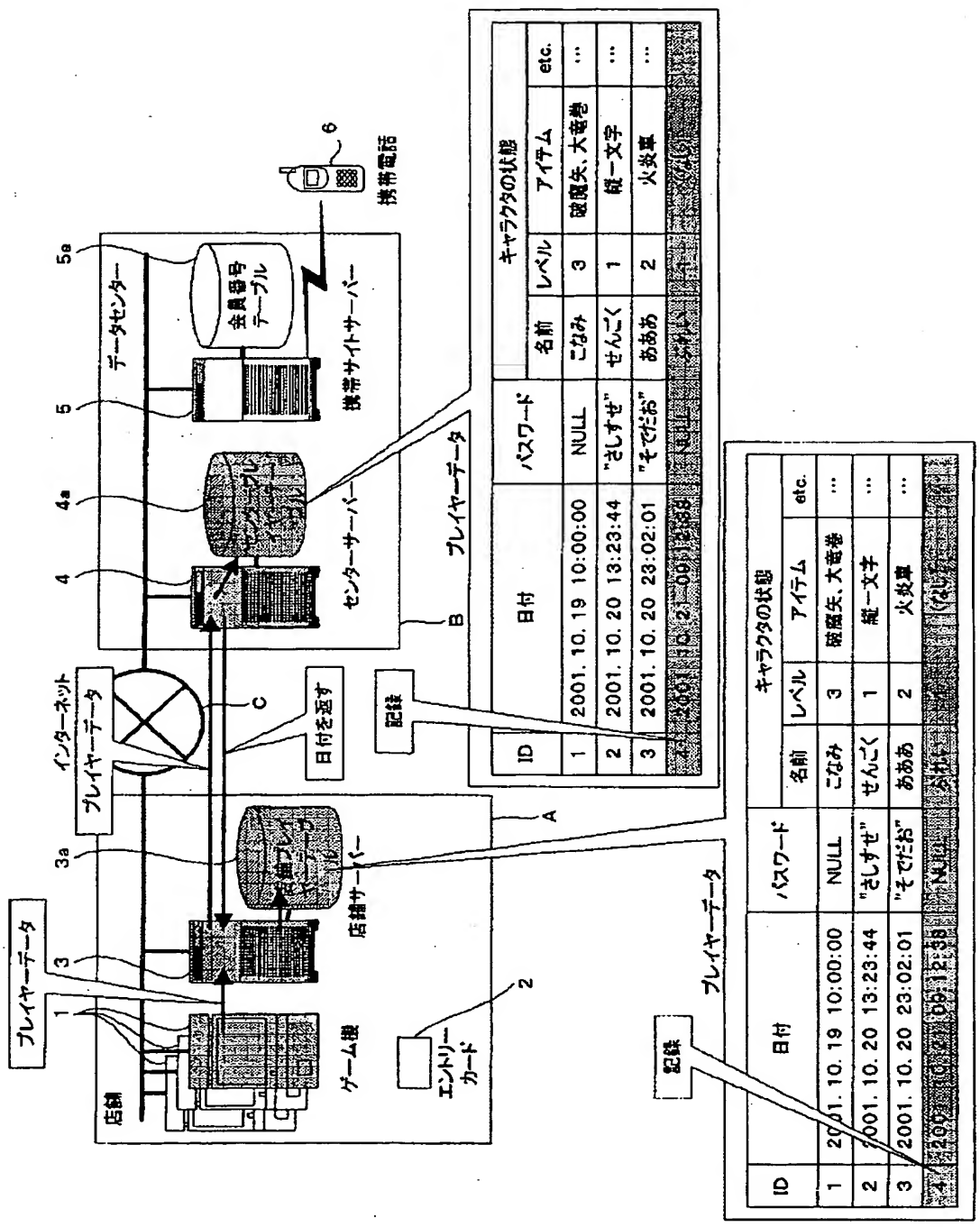
【図１３】


ID発行要求
1
3
3a
インターネット
4
4a
5
5a
店舗
データセンター
店舗プレイヤーテーブル
センタープレイヤーテーブル
会員番号テーブル
C
ゲーム機
店舗サーバー
センターサーバー
携帯サイトサーバー
ID発行、プレイヤーデータ生成
エントリーカード
50
ID書込み
2
A
B
6
携帯電話

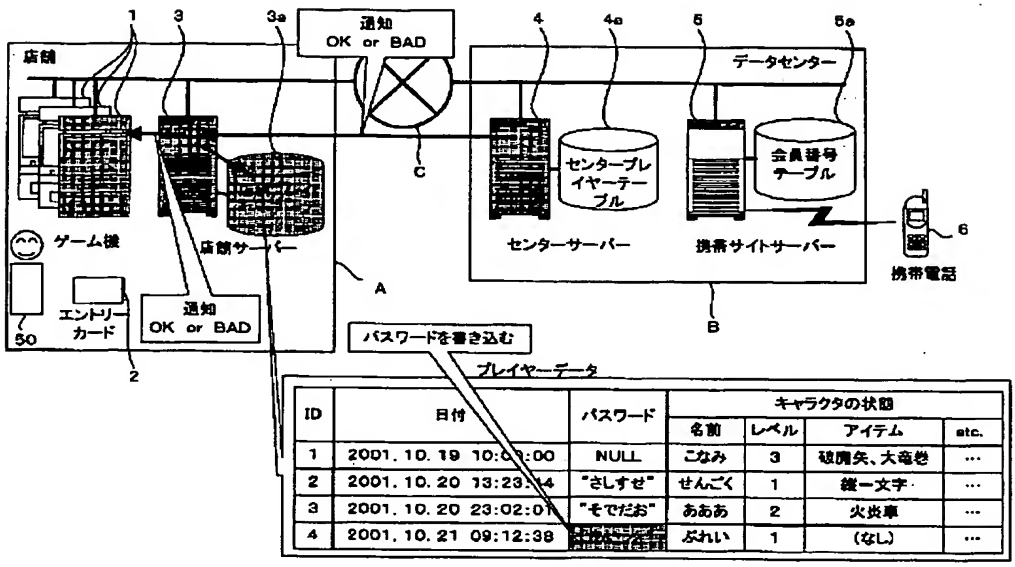
【図１５】


1
3
3a
インターネット
ID+パスワード
4
4a
5
5a
店舗
データセンター
C
店舗プレイヤーテーブル
会員番号テーブル
ゲーム機
店舗サーバー
センターサーバー
携帯サイトサーバー
6
携帯電話
パスワードを書き込む
エントリーカード
ID読取り
B
プレイヤーデータ
60
2
A
パスワード入力「あいうえ」
ID
日付
パスワード
キャラクタの状態
名前
レベル
アイテム
etc.
1 2001. 10. 19 10:00:00 NULL こなみ 3 破魔矢、大吉巻 …
2 2001. 10. 20 13:33:44 "さしすせ" せんごく 1 健一文字 …
3 2001. 10. 20 23:02:01 "そでだお" ああああ 2 火炎草 …
4 2001. 10. 21 09:12:38 ぶれい 1 (なし) …

【図１４】

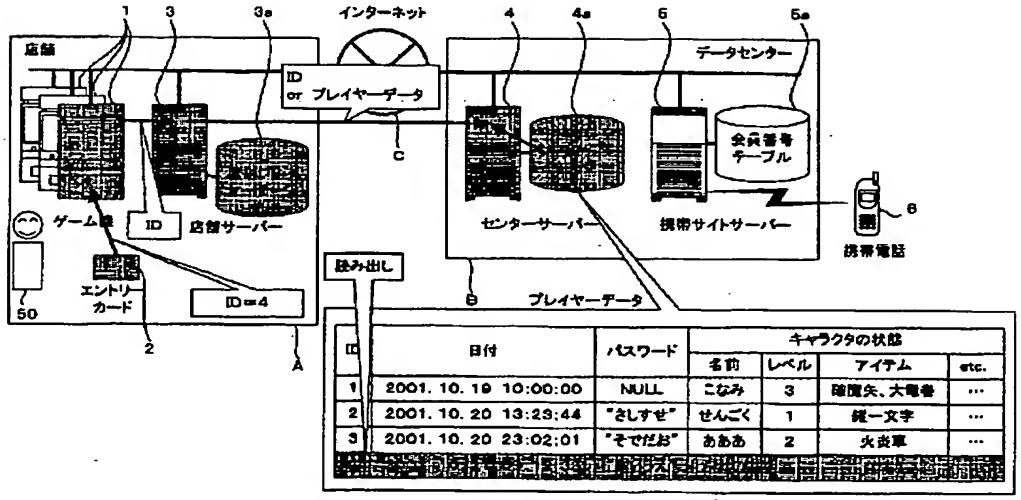

店舗
ゲーム機
エントリーカード
プレイヤーデータ
店舗サーバー
インターネット
プレイヤーデータ
データセンター
センターサーバー
会員番号テーブル
携帯サイトサーバー
携帯電話
日付を返す
記録
プレイヤーデータ
A
B
C
1
2
3
3a
4
4a
5
5a
6
ID
日付
パスワード
キャラクタの状態
名前
レベル
アイテム
etc.
2001. 10. 19 10:00:00
NULL
こなみ
3
破魔矢、大金槌
2001. 10. 20 13:23:44
"さしすせ"
せんごく
1
縦一文字
2001. 10. 20 23:02:01
"そでだお"
ああああ
2
火炎車

【図１６】



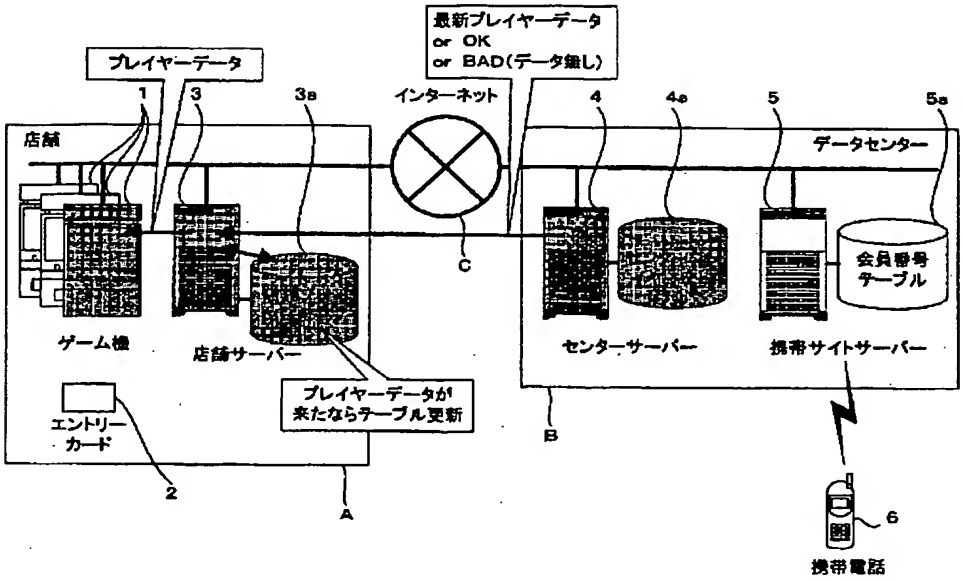
ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大竜巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	ああああ	2	火炎車	…
4	2001. 10. 21 09:12:38		ぶれい	1	(なし)	…

【図１７】



ID	日付	パスワード	キャラクタの状態			
			名前	レベル	アイテム	etc.
1	2001. 10. 19 10:00:00	NULL	こなみ	3	破魔矢、大竜巻	…
2	2001. 10. 20 13:23:44	"さしすせ"	せんごく	1	縦一文字	…
3	2001. 10. 20 23:02:01	"そでだお"	ああああ	2	火炎車	…

【図１８】



フロントページの続き

(72)発明者　中村　勝
東京都港区虎ノ門四丁目３番１号　コナミ
株式会社内

Ｆターム(参考)　2C001 BD04 CB01 CB08
5B085 AA08 AE02 AE03
5K067 AA21 BB04 BB21 DD51 EE02
EE10 EE16 FF02 HH22 HH24
KK13 KK15